More
Happi.

By using the product More Happi, you indicate that you accept the terms of this agreement.

WHEREAS

- The Company provides a coaching platform (“the Platform”) through which the Client’s Employees may book coaching sessions.

- The Client wishes to grant access to the Platform to certain of its Employees (the “Employees”) under the terms set out below.

---

1. Definitions & Interpretation

1.1 Definitions. In this Agreement (unless context requires otherwise):
(a) “Coach” means a volunteer coach contracted by the Company, available via The Platform.
(b) “Employee” means an Employee (or worker) of the Client to whom access is granted.
(c) “Paid Account” means an Employee account permitted to book sessions.
(d) “Platform” means the software application (or service) operated by the Company to view volunteer coaches, manage bookings, user accounts, collect feedback, and related performance data.
(e) “Team” means the collective group of Employees granted access to the platform.
(f) “Base Team Size” means the minimum number of Employees covered under this Agreement for billing purposes (see clause 4).
(g) “Service(s)” means the coaching sessions and ancillary services described in Section 2 of this Agreement or any other contract entered into between the Parties.
(h) “GDPR” means Regulation (EU) 2016/679 and equivalent UK data protection legislation.

1.2 **Interpretation.** Headings are for convenience only. References to clauses, schedules or persons include successors or permitted assigns. “Writing” includes email.

2. Services, Fees & Payments

2.1 **Access & Coaching.**
The Company shall grant the Employees (up to Base Team Size, with agreed increases per clause 4) access to unlimited coaching sessions via the Platform, subject to fair use and scheduling constraints.

2.2 **Coach Supply.**
The Company will provide a pool of available volunteer coaches, onboarded, screened, and trained, available via The Platform.

2.3 **Client Responsibilities.**
(a) The Client shall promptly provide the email addresses of all Employees who will be onboarded and granted access to the Platform.

(b) The Client is responsible for managing (adding, removing) Employee accounts via the Client admin interface. Each email address added to the Platform shall be deemed to represent a paid Seat.

(c) The Client shall ensure that it has an appropriate legal basis for the processing of Employees' personal data for the purposes of providing coaching, feedback, reporting, and any related services

(d) The Client shall use reasonable efforts to encourage Employee engagement (e.g. via communications, reminders).

(e) The Client and its Team agree to provide feedback on the coaching services delivered. Our model relies on this feedback; it supports our volunteer coaches, enables quality assurance, and helps us demonstrate value. The Client commits to encouraging its Team to submit feedback following each session (or when requested) and to support any follow-up call or review as required.

(f) The Client acknowledges that the Company shall not be held financially liable for any technical difficulties or interruptions in service. Any such issues should be reported to hey@morehappi.com, and the Company will use all reasonable efforts to investigate and resolve them promptly.

2.4 **Communications to Employees.**
The Company may send service-related emails to Employees (for example, onboarding notifications, session reminders, content updates, etc.) to support their use of the Platform. The Company may also send weekly educational emails to Employees, covering topics such as learning, development, growth and coaching. Employees will have the option to unsubscribe from these educational communications at any time.

2.5 **Subscription Fees**

Fees depend on your subscription type:

- **Annual Membership:** The terms of your contract, which you have signed, applies. These can be found in your signed contract.

- **Monthly Membership:** You will be charged a monthly fee plus VAT to the payment method registered in the system. Monthly memberships are auto-collected. Charges are based on **seats added to the platform**, not activated seats. You may add or remove team members at any time, and billing will adjust accordingly.

Cancellation & Payments

You acknowledge and agree that More Happi is authorised to charge the payment method used for your initial subscription or any other payment method you have provided. Monthly subscription fees will continue to be billed until the subscription is cancelled. You may cancel at any time; however, cancellation must occur **before the renewal date** to avoid billing for the following month. Refunds are **not available** for partial-month subscription periods.

Fee Adjustments

The Company reserves the right, at its sole discretion, to modify the prices of services or goods provided under this Agreement in line with official inflation rates published by the Bank of England. Adjustments may occur annually or more frequently, as deemed necessary, and will be proportionate to the rate of inflation at the time. Written notice of any price adjustments will be provided to the Client.

For clarity, “inflation” refers to the percentage change in the Consumer Prices Index (CPI) as published by the Office for National Statistics (ONS), or any successor index. Nothing in this clause prevents the Company from adjusting prices based on market conditions or other factors, provided that such increases comply with this Agreement and applicable UK law.

The Company reserves the right to apply interest and late payment charges in line with the Late Payment of Commercial Debts (Interest) Act 1998 and to suspend access to the Platform until payment is received.

3. Nature, Limits & Coach Relationships

3.1 **Non-therapeutic nature.**
(a) Coaching is intended to facilitate the development of personal or professional goals and to develop a plan, strategy or way to achieve those goals. The Client acknowledges that deciding how to handle any issues is the Employee's responsibility.
(b) Coaching is not counselling, psychotherapy, mental health treatment, medical advice, substance abuse treatment, or legal advice.

(c) If a Coach reasonably believes that an Employee may benefit from therapeutic or medical intervention, the Coach may recommend appropriate referral but may not act as a therapist.
(d) The Employee is responsible for their own decisions, mental well-being, and actions.

3.2 **Volunteer Coach Status.**
(a) Coaches are volunteers, not Employees or agents of the Client.
b)The Client acknowledges that the Company's volunteer coaches are based in the UK and have completed accredited coaching training recognised by the ICF, EMCC, or AC. Each coach has documented a minimum of 50 hours of paid and/or volunteer coaching experience.
(c) Volunteer coaches are not remunerated; they volunteer to gain experience as part of the Company accelerator programme in order to gain experience and further industry accreditation.
(d) Volunteer coaches must abide by a separate Coach Agreement with the Company, which includes obligations (e.g. confidentiality, data protection, testimonial usage, brand usage).
(e) Volunteer coaches will have email access to Employees to enable the successful delivery of booked sessions.

3.3 **Testimonials & Branding Permissions.**
(a) The Company may use anonymised testimonials and the Client's logo to show that the Company are a supplier. The Company also permits its volunteer coaches to use anonymised testimonials and the Client's logo for their own marketing purposes.

4. **Confidentiality**

Each party shall treat as confidential all information (commercial, technical, personal, financial) disclosed by the other which is not publicly known, and shall not use or disclose such information except to fulfil its obligations under this Agreement or with prior written consent, or as required by law.

5. Liability & Indemnity

5.1 **Limitation of Liability.**
(a) Subject to the exceptions below, the Company's total liability under all claims in any 12-month period shall not exceed the total fees paid by the Client in that period.
(b) In no event shall the Company be liable for indirect, special, consequential losses, lost profits, business interruption, or reputational loss.
(c) The limitation in (a) applies also to negligence (except for death or personal injury, which cannot be excluded).
(d) The foregoing limitations do not apply to liability arising from fraud, wilful misconduct, or gross negligence.

5.2 **Indemnity.**
The Client shall indemnify the Company (and its directors, officers, volunteer coaches) against claims, losses or liabilities incurred due to the Client's breach (e.g. misuse of platform, data misuse, defamation)

5.3 **Insurance.**
The Company shall maintain appropriate professional indemnity and public liability insurance. The Client may request evidence of such insurance on reasonable notice.

6. Data Protection & Data Processing Agreement

6.1 The DPA in Schedule 1 is incorporated by reference and forms part of this Agreement. In conflict, the DPA prevails for data protection matters.

6.2 The Company acts as data Processor for Employee personal data in connection with the Services.

7. Miscellaneous

7.1 **Notices.** All notices must be in writing (email qualifies). Notices to Company: Hey@morehappi.com. Notices to Client at the address above.

7.2 **Assignment.** Neither party may assign this Agreement (or its rights) without prior written consent (not to be unreasonably withheld).

7.3 **Amendments.** Any amendment must be in writing and signed by authorised representatives.

7.4 **Severability.** If any provision is invalid or unenforceable, it will be severed, and the rest will remain in force.

7.5 **Governing Law & Jurisdiction.** This Agreement is governed by English law. The parties submit to the exclusive jurisdiction of the English courts.

7.6 **Amendments.** The Company may suggest amendments or modifications to this Agreement, including the DPA at any time by posting a revised version at https://morehappi.com. The Company will provide you with notice whenever such amendments are material.

SCHEDULE 1 — Data Processing & Security (DPA)

Data Processing Agreement

This Data Processing Agreement (the “**DPA**”) supplements the More Happi Terms and Conditions, or other agreement in place between you and More Happi ltd covering your use of More Happi Ltd services (the “**Agreement**”). By executing the Agreement, you enter into this DPA on behalf of yourself and, to the extent required under applicable Data Protection Laws (defined below), in the name and on behalf of your affiliates, if any. This DPA incorporates the terms of the Agreement, and any terms not defined in this DPA shall have the meaning set forth in the Agreement.

We may periodically update this DPA by modifying any part or all of the DPA and posting a revised version at https://morehappi.com/. The revised version will become effective and binding the next business day after it is posted.

Terms not defined herein shall have the meaning as set forth in the Agreement.

WHEREAS:

A. Your Company acts as a Data Controller (the “**Controller**”, “**you**”, “**your**”).

B. Your Company wishes to subcontract certain Services (as defined below), which imply the Processing of Company Personal Data, to More Happi ltd, acting as a Data Processor (the “**Processor**”, “**we**”, “**us**”, “**our**”).

C. The Parties seek to implement a data processing agreement that complies with the requirements of the Data Protection Laws.

D. The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. **Definitions and Interpretation**

1.1. “Company Personal Data” means any Personal Data processed by the Processor on Controller’s behalf pursuant to or in connection with the Agreement;

1.2. “Data Protection Laws” means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.3. “EEA” means the European Economic Area;

1.4. “UK/EU Data Protection Laws” means, as applicable to the processing of Personal Data under this Agreement, including 1) GDPR; 2) the EU GDPR as it forms part of the law of

England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR"); and 3) the Data Protection Act 2018;

1.5. “GDPR” means EU General Data Protection Regulation 2016/679;

1.6. “Data Transfer” means: a transfer of Company Personal Data from Controller to a Processor; or an onward transfer of Company Personal Data from a Processor to a Sub-Processor, or between two establishments of a Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.7. “Sub-Processor” means any person appointed by or on behalf of the Processor to process Company Personal Data on behalf of the Controller in connection with the DPA.

1.8. The terms, “Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processing” and “Supervisory Authority” shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. **Processing of Company Personal Data**

2.1. The Processor will only process the Company Personal Data in accordance with Controller’s written instructions specified in Schedule 2. Processor will not process the Company Personal Data for any other purpose or in a way that does not comply with this DPA or Data Protection Laws. Processor must promptly notify Controller if, in its opinion, Controller’s instructions would not comply with Data Protection Laws.

2.2. Processor must promptly comply with any of Controller’s requests or instructions requiring Processor to amend, transfer, delete or otherwise process Company Personal Data, or to stop, mitigate or remedy any unauthorised Processing.

2.3. Processor will maintain the confidentiality of all Company Personal Data and will not disclose the Company Personal Data to third parties unless Controller or this DPA specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires Processor to process or disclose the Company Personal Data, Processor must first inform Controller of the legal or regulatory requirement and give Controller an opportunity to object or challenge the requirement, unless the law prohibits such notice.

2.4. Processor will reasonably assist Controller with meeting Controller’s compliance obligations under Data Protection Laws, taking into account the nature of Processor’s Processing and the information available to Processor, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with Supervisory Authorities under the Data Protection Laws.

2.5. Processor must promptly notify Controller of any changes to Data Protection Laws that may adversely affect Processor’s performance of the Agreement.

2.6. Controller instructs Processor to process Company Personal Data to provide the Services and related technical support.

3. **Processor Personnel**

3.1. Processor shall take reasonable steps to ensure the reliability of any Employee, agent or contractor of any Sub-Processor who may have access to Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with applicable laws in the context of that individual's duties to the Sub-Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

3.2. Processor will ensure that all its Employees with access to the Company Personal Data:

3.2.1. are informed of the confidential nature of the Company Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Company Personal Data;

3.2.2. have undertaken training on the Data Protection Laws relating to handling Company Personal Data and how it applies to their particular duties; and

3.2.3. are aware of both Processor's duties and their personal duties and obligations under the Data Protection Laws and this DPA.

3.3. Processors will take reasonable steps to ensure the reliability, integrity and trustworthiness of the Employees with access to the Company Personal Data.

4. **Security**

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

4.2. Processor must at all times implement appropriate technical and organisational measures against unauthorised or unlawful Processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Company Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Company Personal Data.

4.3. Controller hereby confirms that organisational and technical measures specified in Schedule 2 are sufficient and appropriate under the Data Protection Laws and this DPA.

5. **Sub-processing**

5.1. Processor may not authorise a third party (Sub-Processor) to process the Company Personal Data unless all of the following conditions are met:

5.1.1. Controller has given a specific or general written authorisation to the engagement of the Sub-Processor.

5.1.2. Processor enters into a written contract with each of the authorised Sub-Processors that contains terms substantially the same as those set out in this DPA, in particular, in relation to requiring appropriate technical and organisational data security measures.

5.1.3. At Controller’s request, Processor shall provide a copy of such a sub-Processor agreement and any subsequent amendments to Controller. To the extent necessary to protect business secrets or other confidential information, including Company Personal Data, Processor may redact the text of the agreement prior to sharing the copy.

5.1.4. The Processor maintains control over all Company Personal Data it entrusts to the Sub-Processors.

5.2. The Controller hereby provides a general authorisation for the Processor to engage Sub-Processors to process Company Personal Data under this DPA. The list of authorised Sub-Processors is set out in Schedule 2. Where the Processor intends to update this list, it shall notify the Controller in advance and provide sufficient information to enable the Controller to exercise its right to object. The Controller may object to the engagement of a new Sub-Processor within thirty (30) days of receiving such notice. **If the Controller does not raise an objection within this period, its silence shall be deemed to constitute consent to the proposed Sub-Processor.**

5.3. Where the Sub-Processor fails to fulfil its obligations under such written agreement, the Processor remains fully liable to the Controller for the Sub-Processor’s performance of its obligations.

6. **Data Subject Rights**

6.1. Taking into account the nature of the Processing, Processor shall assist Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Controller obligations, as reasonably understood by Controller, to respond to any complaint, notice, communication or Data Subject request in connection with Company Personal Data processed.

6.2. Processor shall, at reasonable cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to Controller as Controller may reasonably require, to enable Controller to comply with:

6.2.1. the rights of Data Subjects under the Data Protection Laws, including subject access rights, the rights to rectify and erase Company Personal Data, object to the Processing and automated Processing of Company Personal Data, and restrict the Processing of Company Personal Data; and

6.2.2. information or assessment notices served on Controller by any supervisory authority under the Data Protection Laws.

6.3. Processor must notify Controller immediately and without undue delay if it receives any complaint, notice or communication that relates directly or indirectly to the Processing of the Company Personal Data or to either party's compliance with the Data Protection Laws.

6.4. Processor must notify Controller without undue delay when it receives a request from a Data Subject for access to their personal data or to exercise any of their related rights under the Data Protection Laws. Processor shall ensure that it does not respond to that request except on the documented instructions of Controller or as required by applicable laws to which the Processor is subject, in which case Processor shall to the extent permitted by applicable laws, inform Controller of that legal requirement before the Processor responds to the request.

7. **Personal Data Breach**

7.1. The Processor will immediately and without undue delay notify the Controller if it becomes aware of any Personal Data Breach.

7.2. Where Processor becomes aware of the Personal Data Breach, it shall, without undue delay, also provide Controller with the following information:

7.2.1. description of the causes and nature of the Personal Data Breach, including the categories and approximate number of both Data Subjects and Company Personal Data records concerned;

7.2.2. the likely consequences; and

7.2.3. description of the measures taken or proposed to be taken to address (a) and/or (b), including measures to mitigate its possible adverse effects.

7.3. Immediately following any Personal Data Breach, the parties will coordinate with each other to investigate the matter. Processor will reasonably cooperate with Controller in Controller's handling of the matter, including:

7.3.1. assisting with any investigation;

7.3.2. taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Company Personal Data Processing.

7.4. Processor will not inform any third party of any Personal Data Breach without first obtaining Controller's prior written consent, except when required to do so by law.

Processor agrees that Controller has the sole right to determine:

7.5. whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in Controller's discretion, including the contents and delivery method of the notice; and

7.5.1. whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

8. **Data Protection Impact Assessment and Prior Consultation**

Processor shall provide reasonable assistance to Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Sub-Processors.

9. **Deletion or return of Company Personal Data**

9.1. On termination of the Agreement for any reason or expiry of its term, Processor will promptly and in any event within 30 business days securely delete or destroy or, if directed in writing by Controller, return and not retain, all or any Company identifiable information related to this DPA in its possession or control.

9.2. Upon the request from the Controller, Processor will certify in writing that it has deleted the Company identifiable information.

9.3. If any law, regulation, or government or regulatory body requires Processor to retain any documents or materials that Processor would otherwise be required to return or destroy, it will notify Controller in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

10. **Audit rights**

10.1. If Controller is required to show its compliance with Data Protection Laws, reasonably believes that a Personal Data Breach occurred or is occurring, or Processor is in breach of any of its obligations under this DPA or any Data Protection Laws, Processor will permit an assigned and eligible third-party representative of the Controller to audit Processor’s compliance with this DPA obligations, on at least 30 days’ notice, during the Term hereof. The Processor will give the third-party representative of the Controller all necessary assistance reasonably required to conduct such audits. The assistance may include:

10.1.1. physical access to, remote electronic access to any information held at Processor’s premises or on systems storing Company Personal Data;

10.1.2. access to and meetings with any of Processor’s personnel reasonably necessary to provide all explanations and perform the audit effectively; and

10.1.3. necessary inspection of all infrastructure, electronic data or systems, facilities, equipment or application software used to store, process or transport Company Personal Data.

10.2. Information and audit rights of Controller only arise under section 10.1 to the extent that the DPA does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Laws.

10.3. Controller will cover all reasonable expenses incurred by Processor in connection with performing its obligations under clause 10.1.

11. **Data Transfer**

11.1. Controller hereby authorises Processor to transfer or otherwise process Company Personal Data outside the European Economic Area (EEA) or the UK, subject to conditions laid down in this section.

11.2. Processor may only process, or permit the Processing, of Company Personal Data outside the EEA under one of the following conditions:

11.2.1. Processor is processing Company Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Laws that the territory provides adequate protection for the privacy rights of individuals. Processor must identify in an additional annex hereto the territory that is subject to such an adequacy finding;

11.2.2. The Processor takes, where appropriate, one of the safeguards specified by Data Protection Laws, notably by Article 46 of the GDPR.

11.3. If any Company Personal Data transfer between Controller and Processor requires the execution of the Standard Contractual Clauses or the International Data Transfer Agreement in order to comply with the Data Protection Laws (where Controller is the entity exporting Company Personal Data to Processor outside the EEA/UK), the parties will complete all relevant details and take all other actions required to legitimise the transfer.

12. **General Terms**

12.1. **Confidentiality.** Each Party must keep any information it receives about the other Party and its business in connection with this DPA (the "**Confidential Information**") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that (i) disclosure is required by law; and (ii) the relevant information is already in the public domain.

12.2. **Notices.** All notices and communications given under this DPA must be in writing and will be sent by email. Controller shall be notified by email sent to the address related to its use of the Service under the Agreement. The Processor shall be notified by email sent to the address: hey@morehappi.com.

12.3. **Term.** This DPA will remain in full force and effect so long as: (i) the Agreement remains in effect; or (ii) Processor retains any Company Personal Data related to the Agreement in its possession or control (the "**Term**").

13. Governing Law and Jurisdiction. This DPA shall be governed by and construed in accordance with the laws of England and Wales. The parties irrevocably submit to the exclusive jurisdiction of the courts of England and Wales in respect of any dispute arising out of or in connection with this DPA."

Schedule 2: Data Processing and Security

Description of the data Processing carried out on behalf of the Controller.

In addition to the information provided elsewhere in the DPA, the Parties wish to document the following information in relation to the data Processing activities.

The Company Personal data Processing performed by the Processor on behalf of the Controller relates to the provision of the Services as described in the Agreement. The details of the data Processing are as follows:

Subject-matter of Processing:

Coaching services and related emails services provided to Employees of the Controller, as further described in the DPA.

Nature of Processing: The nature of Processing the Company Personal Data under this DPA includes the creation and management of online accounts on the More Happi platform for the Employees of our clients. These accounts are designed to facilitate the booking of coaching sessions with our network of volunteer coaches, who are bound by data processing agreements to ensure the confidentiality and integrity of the data. When an Employee books a session, the information shared with the assigned coach includes the Employee’s name, email address, the Company they are employed by, and the broad theme of the coaching required to tailor the session to the Employee’s needs.

The nature of Processing implies the set of operations such as collection, recording, organisation, structuring, usage, storage, erasure or destruction which is performed on Company Personal Data.

Duration of Processing: The term of the Agreement.

Company Personal Data Categories: Name, email address, date of coaching sessions taken, coach who provided that coaching session, rating of that coaching session, feedback about the coaching session, and testimonial about the coaching session.

Data Subject Types: Employees of the Controller.

Sub-Processors involved:

Name	Services provided	Location

HubSpot	CRM	US
Google	Google Workspace	US
Retool	Code platform	Germany
Planetscale	Database platform	US
Amazon Web Services	Cloud Storage Services	Ireland

Security measures of Processor

The Processor has in place the following technical and organisational data security measures:

Physical access controls

We are a fully distributed Company,. So we have no physical access control needs. When working in public areas, it is Company policy not to leave any Company documents or devices containing Company documents unattended.

System access controls

We use RBAC to ensure that staff members only have access to the permissions to perform the tasks which lie within their job descriptions.
The admin of a system is either a Company director or the head of the department that the tool falls into
We revoke access to any Employee or contractor who leaves us or no longer needs access to a tool to fulfil their duties.

Data access controls

Employees are given access to the data they require to fulfil their standard duties. These duties may be extended from time to time to help ensure coverage of all systems during absences.
We use POLP to ensure that only the necessary data is shown.

Transmission controls

In our app: Our data is both encrypted at rest and in transit.

Input controls

We perform both client side and server side input controls. We do the standard verification of data types, ranges and validity upon entering and then again before writing to our database.
We use a bearer token style authentication and use JWTs to mitigate the risk of man in the middle attacks by verifying the data is signed upon sending and receiving to our servers.

Data backups

Data is backed up at least every 24 hours. In the case of expected risk (a large feature release, an expectation of a large amount of data to flow in a short period), we will increase the number of backups as we deem necessary to mitigate against any data loss.

Data segregation

We don’t store or process enough personal data to have a need to segregate. The two exceptions are:

No payment details are stored within our systems or ever touch our servers. We use Chargebee (a SOC2 Type II compliant service) to store and process payment details.

Passwords and Authentication are handled by AWS Cognito, which has controls around encryption rules and requirements on email verification and password rotation enabled.