

Data Processing Agreement

Club standard form. Fields shown in square brackets are completed by the Brand.

Between: Club AS, a company registered in Norway (organisation number 927 092 026), of Eilert Sundts gate 41, 0355 Oslo, Norway ("**Club**")

And: [Brand legal name], a company registered in [jurisdiction] (company number [company number]), of [registered office address] ("**the Brand**")

This Data Processing Agreement ("**this DPA**") is **Schedule 3** to the Master Services Agreement between the parties (the "**Agreement**"), is attached to and forms part of it under clause 2.1 of that Agreement, and takes effect on the same date.

1. Definitions

1.1 In this DPA:

"Applicable Data Protection Law" means, as applicable to a party's processing: (a) the UK GDPR and the Data Protection Act 2018; (b) Regulation (EU) 2016/679 ("**EU GDPR**") and applicable EU member state and EEA implementing law, including as applied in Norway; and (c) the Privacy and Electronic Communications Regulations 2003, in each case as amended or replaced.

"Brand Personal Data" means Personal Data Processed by Club on behalf of the Brand under the Agreement, as described in Annex 1.

"Brand-Recruited User" means an ambassador or user who joined the Brand's programme via an invite link, web embed, newsletter sign-up, manual import or other channel originating with the Brand.

"Club-Discovery User" means an ambassador or user who discovered the Brand through Club's own network, discovery tools or marketplace.

"controller", "processor", "data subject", "Personal Data", "Personal Data Breach", "Process" and "Processing" have the meanings given in Applicable Data Protection Law.

"EU SCCs" means the standard contractual clauses annexed to European Commission Implementing Decision (EU) 2021/914.

"Restricted Transfer" means a transfer of Personal Data to a country or recipient not covered by an adequacy decision or regulation applicable to the transferring party.

"Sub-processor" means any processor engaged by Club to Process Brand Personal Data.

"UK Addendum" means the International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner under s.119A of the Data Protection Act 2018.

1.2 Where this DPA conflicts with any other part of the Agreement in relation to the Processing of Personal Data, this DPA prevails.

2. Structure and allocation of roles

2.1 This DPA has two operative parts, reflecting the two distinct data flows in the Club Platform:

(a) **Part A (sections 3 to 15)** applies where Club acts as **processor** on behalf of the Brand as controller. This covers all Brand Personal Data, including data relating to Brand-Recruited Users, the Brand's own personnel and authorised users, and the Brand's customer data received through eCommerce integration.

(b) **Part B (section 16)** applies where Club and the Brand each act as **independent controllers**. This covers data relating to Club-Discovery Users, and Club's Processing of Platform usage data for its own purposes as set out in section 16.

2.2 Neither party is a joint controller with the other, and nothing in the Agreement creates joint controllership.

2.3 The allocation of roles in this section reflects the factual reality of the Processing. Where a Processing activity is not clearly addressed, the parties shall discuss in good faith and record the agreed allocation in writing.

PART A: CLUB AS PROCESSOR

3. Scope and instructions

3.1 Club shall Process Brand Personal Data only:

(a) for the purposes and by the means set out in Annex 1; (b) on the Brand's documented instructions, which include the Agreement, the Order Form, any applicable service level agreement, configuration choices made by the Brand in the Platform, and any further written instruction given by the Brand; and (c) where required by law, in which case Club shall (unless legally prohibited) inform the Brand before Processing.

3.2 Club shall not Process Brand Personal Data for its own purposes except as set out in section 16.

3.3 Club shall not sell Brand Personal Data or disclose it for cross-context behavioural advertising.

3.4 Club shall promptly inform the Brand if, in Club's opinion, an instruction from the Brand infringes Applicable Data Protection Law. Club may suspend the affected Processing until the instruction is confirmed, withdrawn or amended.

3.5 The Brand warrants that it has a lawful basis for the Processing it instructs, has provided all required transparency information to data subjects, and that its instructions comply with Applicable Data Protection Law.

3.6 Club shall maintain a written record of its Processing of Brand Personal Data sufficient to satisfy Article 30(2) UK GDPR, and shall make it available to the Brand on request.

4. Confidentiality of personnel

4.1 Club shall ensure that access to Brand Personal Data is limited to personnel who need it to perform the Agreement. In this section 4, "personnel" means any individual engaged by Club or by any affiliate of Club, including Brandbassador AS, who has access to Brand Personal Data. Club remains responsible under this Agreement for the acts and omissions of all such individuals as if they were its own.

4.2 Club shall ensure that all such personnel are:

(a) bound by written confidentiality obligations surviving termination of their engagement; and (b) trained in data protection and information security on induction.

4.3 Club shall maintain a record of personnel with access to Brand Personal Data, and shall revoke access promptly on change of role or termination of engagement.

5. Security

5.1 Club shall implement and maintain the technical and organisational measures set out in **Annex 2**, being measures appropriate to ensure a level of security appropriate to the risk, having regard to Article 32 UK GDPR.

5.2 Club may update the measures in Annex 2 from time to time provided that the level of protection is not materially reduced. Club shall notify the Brand of any material change.

5.3 Club shall keep the effectiveness of its security measures under review.

6. Sub-processors

6.1 The Brand gives general written authorisation for Club to engage Sub-processors, subject to this section 6.

6.2 The Sub-processors authorised at the date of this DPA are listed in **Annex 3**. Club maintains its current list of Sub-processors and may make it available online. The list as updated from time to time supersedes Annex 3.

6.3 Club shall:

(a) satisfy itself before engagement that each Sub-processor can provide sufficient guarantees under Article 28(1) UK GDPR; (b) impose on each Sub-processor, by written contract, data protection obligations no less protective than those in this Part A; and (c) remain liable to the Brand for the acts and omissions of its Sub-processors as if they were its own, subject to section 14.

6.4 **Change notification.** Club shall notify the Brand of the addition or replacement of a Sub-processor by updating its list of Sub-processors. The Brand is responsible for reviewing the list from time to time. Notice shall identify the Sub-processor, the Processing it will carry out, the categories of Personal Data involved, and its location.

6.5 **Right to object.** The Brand may object to a Sub-processor on reasonable data protection grounds by written notice within twenty (20) days of the list being updated. The parties shall discuss the objection in good faith and Club shall use reasonable endeavours to make available an alternative arrangement that avoids the Processing objected to.

6.6 Where a change of Sub-processor is required urgently to maintain security or continuity of service, Club may make the change immediately and shall notify the Brand as soon as reasonably practicable, and the Brand's rights under section 6.5 apply from the date of that notice.

7. Data subject rights

7.1 Club shall provide functionality within the Platform, or supported processes, enabling the Brand to access, correct, export, restrict and delete Brand Personal Data.

7.2 Where a data subject makes a request to Club that relates to Brand Personal Data, Club shall not knowingly respond substantively (other than to acknowledge and to direct the data subject to the Brand where appropriate) and shall notify the Brand without undue delay and in any event without undue delay after identifying the request as such.

7.3 Club shall provide the Brand with reasonable assistance, at the Brand's cost where the assistance requires material effort beyond standard Platform functionality, to enable the Brand to respond to requests under Articles 15 to 22 UK GDPR within the statutory time limits.

8. Assistance and accountability

8.1 Club shall, at the Brand's cost, provide the Brand with reasonable assistance in:

(a) carrying out data protection impact assessments in respect of the Processing under this DPA, including by providing information about Club's Processing operations, security measures and Sub-processors; and (b) any prior consultation with a supervisory authority arising from such an assessment.

8.2 Club shall notify the Brand without undue delay if it receives any complaint, enquiry, investigation notice or other communication from a supervisory authority that relates to the Processing of Brand Personal Data, and shall provide reasonable assistance to the Brand in responding, at the Brand's cost.

8.3 Where Club receives a legally binding request from a public authority for disclosure of Brand Personal Data, Club shall (unless legally prohibited):

(a) notify the Brand without undue delay; (b) challenge any request that is unlawful, overbroad or not made in accordance with due process; and (c) disclose only the minimum data legally required.

9. Personal Data Breach

9.1 Club shall notify the Brand of any Personal Data Breach affecting Brand Personal Data without undue delay after becoming aware of it.

9.2 The notification shall include, to the extent known at the time and updated as further information becomes available:

(a) a description of the nature of the breach; (b) the categories and approximate number of data subjects and records affected; (c) the likely consequences; (d) the measures taken

or proposed to address the breach and mitigate its effects; and (e) the name and contact details of Club's point of contact.

9.3 Club shall not delay the initial notification in order to complete its investigation. Where full information is not available, Club shall provide what is known and supply the remainder in phases without further undue delay.

9.4 Club shall:

(a) take all reasonable steps to contain, investigate and remediate the breach; (b) preserve evidence and maintain a written record of the breach and its response; (c) provide the Brand with all information the Brand reasonably requires to meet its own notification obligations under Articles 33 and 34 UK GDPR; and (d) provide, on the Brand's written request, a summary of the cause of the breach and the steps taken, at the Brand's cost.

9.5 Club shall not notify any third party, data subject or supervisory authority of a Personal Data Breach affecting Brand Personal Data in terms that identify the Brand, without the Brand's prior written approval, unless and to the extent Club is required to do so by law. Where Club is a controller of data affected by the same incident under Part B, this section does not restrict Club from discharging its own notification obligations as controller, and the parties shall coordinate their communications so far as practicable.

10. Deletion and return

10.1 On the Brand's written request at any time, and in any event within sixty (60) days of expiry or termination of the Agreement, Club shall at the Brand's election either return Brand Personal Data to the Brand in a structured, commonly used, machine-readable format, or securely delete it.

10.2 Where the Brand requests return, Club shall provide the data within sixty (60) days and shall then delete it in accordance with section 10.1.

10.3 Club may retain Brand Personal Data to the extent and for so long as required by law, and shall in that case:

(a) notify the Brand of the data retained, the legal basis and the retention period; and (b) continue to apply this DPA to that data for as long as it is retained, Processing it only for the purpose requiring its retention.

10.4 Club shall confirm deletion in writing on the Brand's request.

10.5 Nothing in this section requires Club to delete Personal Data relating to Club-Discovery Users, which Club Processes as controller under Part B, or data lawfully retained under Club's own retention policy in its capacity as controller. Club shall on request confirm which categories of data it continues to hold and on what basis.

10.6 Club's standard retention periods for Brand Personal Data are set out in Annex 1.

11. Audit and information rights

11.1 Club shall make available to the Brand such information as Club holds that is reasonably necessary to demonstrate compliance with this Part A, including:

(a) the security measures in Annex 2 and any updates; (b) any summary of security review Club holds under section 5.3; (c) its current Sub-processor list and a summary of the data protection terms in place with Sub-processors; (d) its record of Processing under section 3.6; and (e) any third-party certification, audit report or assessment summary Club holds.

11.2 Where the information provided under section 11.1 is not sufficient to demonstrate compliance, the Brand may audit Club's Processing of Brand Personal Data, subject to the following:

(a) not more than once in any twelve (12) month period, save where required by a supervisory authority; (b) on at least sixty (60) days' written notice; (c) during Business Hours, and conducted so as to minimise disruption to Club's operations; (d) by the Brand or an independent auditor appointed by the Brand who is not a competitor of Club and who is bound by confidentiality obligations; (e) not extending to any data, system or premises relating to Club's other customers; and (f) at the Brand's cost.

11.3 Club shall remediate any material non-compliance identified by an audit within a reasonable period agreed with the Brand.

12. International transfers

12.1 Club shall not make a Restricted Transfer of Brand Personal Data unless it has put in place a transfer mechanism valid under Applicable Data Protection Law.

12.2 The transfers taking place at the date of this DPA, and the mechanism applicable to each, are set out in **Annex 4**.

12.3 Where a Restricted Transfer from the UK is required and no adequacy regulation applies, the parties agree that the **EU SCCs as amended by the UK Addendum** are incorporated into this DPA by reference, on the following basis:

(a) **Module Three (processor to processor)** applies, with Club as data exporter and the relevant Sub-processor as data importer. Where a transfer is made directly by the Brand as controller, **Module Two** applies, with the Brand as data exporter and Club or the relevant Sub-processor as data importer; (b) the optional docking clause (Clause 7) applies; (c) in Clause 9, **Option 2 (general written authorisation)** applies, with the notice period in section 6.4 of this DPA; (d) in Clause 11, the optional independent dispute resolution language does not apply; (e) in Clause 17, the governing law is the law of England and Wales; (f) in Clause 18(b), the forum is the courts of England and Wales; (g) Annexes I, II and III to the EU SCCs are populated by Annexes 1, 2 and 3 to this DPA respectively; and (h) Table 4 of the UK Addendum: neither party may end the Addendum as set out in section 19 of the Mandatory Clauses.

12.4Where a Restricted Transfer from the EEA or Norway is required, the **EU SCCs** apply on the equivalent basis, with the governing law and forum being those of Norway.

12.5Where Club acts as data exporter in respect of a Restricted Transfer to a Sub-processor, Club shall enter into the applicable clauses with that Sub-processor and shall carry out a transfer risk assessment where required by Applicable Data Protection Law. Club shall make any such assessment available to the Brand on request.

12.6Where a transfer mechanism relied on is invalidated, or a supervisory authority or court determines it may not lawfully be used, Club shall without undue delay implement an alternative lawful mechanism or, where none is available, cease the affected transfer. Where neither is possible and the affected Processing is material to the Services, either party may terminate the affected Services on written notice, and Club shall refund fees paid in respect of any period after termination.

13. Special category data

13.1Other than the categories of Personal Data described in Annex 1, the Brand shall not instruct Club to Process, and shall not upload to the Platform, any special category Personal Data within the meaning of Article 9 UK GDPR (including data concerning health) or criminal offence data within the meaning of Article 10, except with Club's prior written agreement and subject to any additional measures the parties agree.

13.2Club's Platform is not designed to Process special category Personal Data, and Annex 2 describes measures appropriate to the categories of data in Annex 1.

13.3The parties acknowledge that the Brand operates in the health sector and that ambassador and customer data may permit inferences about the health of a data subject. The parties shall discuss and agree in writing before Processing begins any additional measures required in respect of: (a) product-level purchase or order data received through eCommerce integration; and (b) any mission, submission or content that may reveal such information about a data subject. Measures agreed under this section shall be recorded in Annex 1 and, where they concern security, Annex 2.

14. Liability

14.1This DPA does not create any liability additional to that provided for in the Agreement. The limitations and exclusions of liability in the Agreement apply to this DPA as if set out in it in full, and apply to all claims under or in connection with this DPA. Where the Agreement does not limit liability for a matter arising under this DPA, each party's aggregate liability for that matter shall not exceed one hundred per cent (100%) of the fees paid or payable under the Agreement in the twelve (12) months preceding the first event giving rise to it.

14.2 Neither party is liable for loss of profit, loss of revenue, loss of anticipated savings, loss of business or any indirect or consequential loss arising under or in connection with this DPA.

14.3 Nothing in this DPA limits or excludes any liability that cannot lawfully be limited or excluded.

14.4 Where the parties are liable to a data subject for the same damage, each shall bear liability in proportion to its responsibility for the damage, and each shall be entitled to claim back from the other any amount paid in excess of its share.

15. Term

15.1 Part A takes effect on the Effective Date of the Agreement and continues for so long as Club Processes Brand Personal Data, notwithstanding expiry or termination of the Agreement.

PART B: THE PARTIES AS INDEPENDENT CONTROLLERS

16. Independent controller processing

16.1 The parties acknowledge that each acts as an independent controller in respect of:

(a) **Club as controller:** the identity and contact details of Club-Discovery Users, Club's ambassador network and community data, identity and payment verification data for ambassador reward payments, aggregated or anonymised Platform usage and performance data Processed by Club for the purposes of operating, securing, analysing and improving the Club Platform and its network, and the business contact details of the Brand's personnel together with records of Club's dealings with them, including notes, correspondence and recordings and transcripts of meetings, Processed by Club for the purposes of managing the customer relationship. Club shall inform the Brand's personnel where a meeting is recorded;

(b) **the Brand as controller:** Personal Data the Brand obtains through the Platform and then Processes for its own purposes outside the Platform, including the contact details of Brand-Recruited Users which the Brand is permitted to use outside the Platform.

16.2 Each party shall, in respect of its own controller Processing:

(a) comply with Applicable Data Protection Law; (b) maintain a lawful basis for its Processing; (c) provide the transparency information required by Articles 13 and 14 UK GDPR to the data subjects concerned; (d) implement appropriate technical and organisational measures under Article 32; (e) respond to data subject requests made to it, and pass to the other party without undue delay any request that party is better placed to answer; and (f) fulfil its own breach notification obligations to supervisory authorities and data subjects.

16.3 The Brand shall not extract, export or attempt to harvest the contact details or external identifiers of Club-Discovery Users, and shall not Process such data for any purpose outside the Platform.

16.4 Where one party's act or omission causes the other to breach Applicable Data Protection Law, the party at fault shall provide reasonable assistance to the other in responding.

16.5 Each party shall notify the other without undue delay of any Personal Data Breach affecting its own controller Processing where the breach is reasonably likely to affect the other party's data subjects or require the other party to notify, and the parties shall coordinate their communications so far as practicable.

16.6 Neither party shall represent to any data subject, supervisory authority or third party that the parties are joint controllers.

17. Governing law

17.1 This DPA is governed by the law of England and Wales, and the parties submit to the exclusive jurisdiction of the courts of England and Wales, save where the EU SCCs require otherwise in respect of a specific transfer.

Signatures

For Club	For the Brand
Signature:	Signature:
Name: Thomas Adams	Name:
Title: Chief Executive Officer	Title:
Date:	Date:

ANNEX 1: DETAILS OF PROCESSING

A. Subject matter and duration

The subject matter is Club's provision of the Club Platform and related services under the Agreement. Processing continues for the Term and for the periods in section E below.

B. Nature and purpose of the Processing

Activity	Purpose
Hosting and storage of ambassador profiles	Operating the Brand's community on the Platform
Mission creation, distribution and submission review	Delivering the core service
Reward, discount code, gift card and commission processing	Paying and rewarding ambassadors
eCommerce integration	Attributing orders and generating discount codes and affiliate links
Segmentation and analytics	Targeting Missions and reporting performance to the Brand
Notifications, email and in-app messaging	Communicating with ambassadors about the Brand's programme
Support	Handling ambassador and Brand queries

C. Categories of data subject

- Ambassadors and users who are members of the Brand's community, in particular Brand-Recruited Users
- The Brand's personnel and authorised Platform users
- The Brand's customers, where order or customer data is received through eCommerce integration

D. Categories of Personal Data

Category	Detail
Identity and contact	Name, username, email address, postal address, phone number, date of birth, gender, country
Profile	Social media handles and public profile data, follower counts, interests, sizing and demographic attributes supplied by the data subject
Content	Submissions, images, video, posts, wall comments and messages
Behavioural	Mission participation, submission history, engagement and performance metrics, Platform usage

Category	Detail
Commercial	Discount code and affiliate link usage, attributed orders, order value, reward and commission balances
Technical	IP address, device and browser data, online identifiers, cookie identifiers
Payment	Reward and commission balances, payout status, and the payout beneficiary identifier and beneficiary address. Bank account numbers and payout credentials are held by the payment provider named in Annex 3 and are not stored by Club
Identity verification	The outcome of the verification only. Identity documents are captured and held by the identity verification supplier named in Annex 3 and are not stored by Club
Customer data via eCommerce integration	Order identifier, timestamp, order total and, where enabled by the Brand, customer email address. Club does not store product or SKU level purchase detail. The data stored is limited to the order identifier, timestamp, order total and, where enabled by the Brand, the customer email address

E. Retention

Data	Period
Ambassador account and profile data	For the life of the account, then 24 months after last activity
Mission submissions and content	For the Term, then deleted with the account or on Brand request
Order and commission records	6 years from the end of the financial year in which the transaction occurred, to meet tax and accounting obligations
Identity and address verification records	6 years from the date of the last payout, to meet anti-money-laundering and payment audit obligations
Support correspondence	24 months from the date of last contact
Security and audit logs	400 days

Deletion. The periods above state the period for which Club undertakes to retain the data and the point from which it may be deleted. Deletion is effected on request by the Brand or the data subject under section 10, and through ambassador self-service in the Platform's account settings. Data held in backup media is overwritten in the ordinary course of Club's backup cycle, within 30 days, and this DPA continues to apply to it until then.

ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES

1. Encryption and key management

Measure	Position
Encryption in transit	All connections to the Platform and its APIs are secured with HTTPS. TLS 1.2 is the minimum version accepted; TLS 1.3 is supported
Encryption at rest	Personal Data is encrypted at rest. Storage is encrypted at the disk level using Google-managed encryption keys, and Personal Data identified as sensitive is further encrypted at the application layer within the event store
Credential storage	User passwords are stored using bcrypt with a per-user salt. Plaintext passwords are never stored
Secret management	Application secrets are held in managed cloud secret storage
Payment data	Bank account and payout credentials are held by the payment provider named in Annex 3. Club stores reward and commission balances and payout status only

2. Access control

Measure	Position
Named accounts	Every Platform user has their own credentials. Shared or generic accounts are not used
Authentication	Administrators are invited by email and set their own password. Login is by email address and password
Federated identity and single sign-on	Not supported
Role-based access control	Four administrator roles with least-privilege scoping: Superadmin (full access including settings, billing and user administration), Admin (all areas except settings), Set-up (settings only, used during integration), Support (support chat only)
Separation of Brand and ambassador environments	Brand administrators operate only in the Brand environment and do not have access to the ambassador environment

Measure	Position
Segregation of Brand data	An ambassador holds a single Platform account and may participate in more than one Brand's programme. Each Brand's view of that ambassador is segregated: a Brand administrator can access only the ambassadors associated with that Brand's own programmes, and only that Brand's mission, submission and commercial data. The Platform provides no route by which one Brand may access another Brand's ambassador list, submissions or commercial data
Account lifecycle	Superadmins can add and remove administrators at any time, so the Brand controls who holds access and can revoke it immediately
Infrastructure access	Access to production infrastructure is controlled through cloud provider identity and access management, and databases sit behind a firewall
Multi-factor authentication	Two-factor authentication is enforced for all Club personnel accessing the cloud infrastructure on which the Platform runs, through the corporate identity provider. The Platform itself and its administrative tooling do not currently support multi-factor authentication for Brand administrators. Access to those is instead controlled by named accounts, role-based scoping, and the Brand's own ability to revoke administrators immediately
Access logging	Access to production data is recorded in audit logs, which are retained for 400 days and are available to investigate any suspected incident. Error logs are monitored as part of normal operations

3. Integrity and development

Measure	Position
Code review	Changes are peer reviewed before release
Vulnerability scanning	Dependency vulnerability scanning runs against the codebase as part of the development pipeline, and all changes are peer reviewed before release
Source code protection	Source code is held in private repositories
Environment separation	Production, staging and development environments are separated. Production data is not used in test environments

4. Availability and resilience

Measure	Position
Hosting	Google Cloud Platform, europe-west1 (Belgium)
Database hosting	Google Cloud Platform, europe-west1 (Belgium). All databases operated by Club are hosted within the European Union
Backups	Two databases are operated. The relational database is backed up daily, retained for 30 days, with 7 days of point-in-time recovery. The event store is backed up hourly, with snapshots retained for 30 days

Measure	Position
Restore testing	The relational database restore path is exercised on every release, approximately fortnightly, because the blue-green deployment process restores from backup to duplicate data. The event store restore was last exercised on 30 August 2024
Recovery point objective	Recovery follows the backup cadence above: up to 1 hour for the event store, and up to 24 hours for the relational database, reducing to near zero within the 7 day point-in-time recovery window
Monitoring	Error logs are monitored as part of normal operations. Audit logs of access to production data are retained for 400 days and are available for investigation

5. Organisational measures

Measure	Position
Accountability	A named individual is accountable for data protection. Contact details are given for the purposes of section 9.2(e): Thomas Adams, Chief Executive Officer, thomas@club.co
Information security governance	Responsibility for information security is held within Club's technical leadership team
Incident response	Club's obligations to notify, investigate and assist in respect of a Personal Data Breach are set out in section 9 and are contractually binding
Staff training	All personnel receive data protection and information security training on induction, covering the handling of personal data, physical device security and the mandatory use of two-factor authentication on company accounts. Training is delivered as part of the induction programme
Confidentiality	All personnel with access to Personal Data are bound by written confidentiality obligations
Infrastructure certification	The Platform is hosted on Google Cloud Platform, which maintains ISO 27001, SOC 2 and other certifications covering the underlying infrastructure
Sub-processor due diligence	Club selects established providers and contracts with them on their standard data protection terms
Record of Processing	Maintained under section 3.6

6. Data minimisation and deletion

Measure	Position
Integration minimisation	The eCommerce integration retrieves only the data required for Platform functionality, principally order data

Measure	Position
Deletion on request	Personal Data is deleted on request by the Brand or the data subject in accordance with section 10
Self-service deletion	An ambassador can delete their own account at any time from the Platform's account settings, without contacting Club
Retention and deletion	Personal Data is deleted on request by the Brand or the data subject under section 10, and an ambassador may delete their own account at any time from the Platform's account settings
Secure disposal	Media disposal is managed by the hosting and infrastructure providers under their own certified processes

ANNEX 3: AUTHORISED SUB-PROCESSORS

Each Sub-processor receives the Personal Data described in the table below for its stated purpose. Access is through that Sub-processor's interface or API, save for the artificial intelligence providers, which receive the content submitted to the features they support.

A. Core Sub-processors

Engaged for all Brands.

Sub-processor	Purpose	Data categories	Location
Google Cloud Platform	Application hosting, database hosting and storage	All categories in Annex 1	EU (europe-west1, Belgium)
Twilio	SMS and messaging	Name, phone number, message content	United States
SendGrid	Transactional and Platform email	Name, email address, message content	United States
OneSignal	Push notifications to ambassadors	User identifiers, device tokens	United States
Intercom	Ambassador support chat	Contact data, support correspondence	United States
Airwallex (UK) Limited	Ambassador reward and commission payouts	Identity, contact, beneficiary and payout data	United Kingdom (Wells and More, 45 Mortimer Street, London W1W 8HJ)
Stripe	Payment processing	Billing contact and payment data	United States and EU
Xero	Accounting	Brand and Brand administrator billing contact data only. Xero does not receive ambassador Personal Data	Outside the UK and EEA
Anthropic	AI features within the Platform, under a business account. Brand Personal Data is not used to train models	Data submitted to AI features	United States

Sub-processor	Purpose	Data categories	Location
AskAI Ltd (MyAskAI)	Automated triage and response in ambassador support	Ambassador support correspondence, contact data	United States
GrowthBook	Feature flagging and experimentation	Email address, user ID, Brand ID, Brand name	United States (Amazon Web Services)
ClientSuccess	Customer success platform	Brand contact names, account records, usage events	United States (Amazon Web Services)
LogRocket	Session replay and front-end diagnostics. Legacy integration, scheduled for removal	Technical and usage data, session recordings	United States
Google Analytics	Platform usage analytics	Technical and usage data, online identifiers	United States and EU
Instabug	In-app bug reporting and diagnostics	Technical and usage data, report content	United States
Jam	Bug reporting and diagnostics	Technical and usage data, report content	United States

B. Optional integrations

Engaged only where the Brand chooses to connect the relevant service.

Sub-processor	Purpose	Data categories	Location
Shopify	eCommerce integration	Order data, discount codes, customer email where enabled by the Brand	United States and Canada
BigCommerce	eCommerce integration	Order data, discount codes, customer email where enabled by the Brand	United States
Centra	eCommerce integration	Order data, discount codes, customer email where enabled by the Brand	Sweden (EU)
Klaviyo	Marketing automation	Name, email address, engagement data	United States
Meta Platforms	Advertising and attribution	Technical and usage data, online identifiers	United States
TikTok	Advertising and attribution	Technical and usage data, online identifiers	United States

C. Ambassador-only Sub-processors

Engaged in respect of individual ambassadors, not in respect of Brand administrators.

Sub-processor	Purpose	Data categories	Location
Jumio	Ambassador identity verification. Identity documents are held by Jumio; Club receives and stores the verification outcome only	Identity documents, verification outcome	EU processing region
IP-API	IP geolocation. Club sends the IP address only	IP address	Outside the UK and EEA

Club shall maintain an up-to-date list and make it available to the Brand on request. Changes are notified under section 6.4.

ANNEX 4: INTERNATIONAL TRANSFERS

Transfer	Exporter	Importer	Destination	Mechanism
Brand to Club	the Brand	Club AS	Norway	Adequacy. Norway is an EEA state and is covered by the UK adequacy regulations, so no standard contractual clauses are required for this transfer
Club to EU Sub-processors	Club AS	Google Cloud Platform, Centra, Jumio (EU region)	EU	Adequacy
Club to UK Sub-processors	Club AS	Airwallex (UK) Limited	United Kingdom	Adequacy. The European Commission's adequacy decision for the United Kingdom covers this transfer
Club to Sub-processors outside the UK and EEA	Club AS	Each Sub-processor in Annex 3 located outside the UK and EEA	Principally the United States	Club relies on the EU SCCs Module Three together with the UK Addendum, or on EU-US Data Privacy Framework certification where the importer is certified. Club shall confirm the mechanism applicable to each Sub-processor on the Brand's request