

# DATA PROCESSING AGREEMENT

**ACCORD DATA PTY LTD**

(Processor)

*Incorporating the Standard Contractual Clauses approved by  
Commission Implementing Decision (EU) 2021/914,  
and the UK International Data Transfer Addendum (version B1.0).*

Version 1.0 — published 24 April 2026  
Canonical URL: <https://accord.gg/legal/dpa>

## How this DPA takes effect

This Data Processing Agreement (the “DPA”) is the standard data-processing contract between Accord Data Pty Ltd (“Accord”, the Processor) and each of its customers (each a “Customer”, the Controller). This DPA is published at <https://accord.gg/legal/dpa> and is incorporated by reference into every Services Agreement, Master Subscription Agreement, Order Form, or other written agreement under which Accord provides the Accord platform and services (the “Services Agreement”).

Customer-specific details — including the Customer’s legal name, registered address, signing authority, effective date, and fees — are set out in the Services Agreement and not repeated in this DPA. Where this DPA refers to the “Customer” or the “Controller”, it means the contracting counterpart identified in the Services Agreement.

A Customer can request a signed counterpart of this DPA at any time by emailing [privacy@accord.gg](mailto:privacy@accord.gg). Signing a counterpart does not change the substantive terms of this DPA; it produces an executed record of the same text.

Accord may update this DPA from time to time. Material changes will be notified to active Customers by email (or via the dashboard) and will take effect no earlier than 30 days after notification. A change log is maintained at the bottom of this document.

## Parties

**(1) ACCORD DATA PTY LTD**, a company incorporated in Australia (ACN 691 164 584; ABN 60 691 164 584), whose registered office is at Suite 3, 99 Musgrave Road, Red Hill, Queensland 4059, Australia (**Accord** or the **Processor**); and

**(2) the Customer** identified in the Services Agreement (the **Customer** or the **Controller**), each a “Party” and together the “Parties”.

## Background

(A) The Parties have entered into, or will enter into, a Services Agreement under which Accord provides the Accord platform and associated services to the Customer.

(B) In the course of performing the Services Agreement, Accord will process personal data on the Customer’s behalf within the meaning of the GDPR and, where applicable, the UK GDPR.

(C) This DPA sets out the terms on which Accord will process personal data, and incorporates by reference the EU Standard Contractual Clauses (Module Two – Controller to Processor) approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the “EU SCCs”) and, where applicable, the ICO’s International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0 (the “UK Addendum”).

(D) This DPA is intended to satisfy the requirements of Article 28 GDPR and, in relation to transfers of personal data outside the EEA and the United Kingdom, to provide appropriate safeguards pursuant to Article 46 GDPR and Article 46 UK GDPR.

## 1. Definitions and Interpretation

1.1 In this DPA, capitalised terms not otherwise defined have the meaning given in the GDPR or, where applicable, the UK GDPR. The following additional definitions apply:

- “GDPR” means Regulation (EU) 2016/679 (General Data Protection Regulation).

- “UK GDPR” means the retained EU law version of Regulation (EU) 2016/679, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, read together with the Data Protection Act 2018.
- “Personal Data” means any personal data processed by Accord on behalf of the Customer under the Services Agreement, as described in Annex I.B.
- “Services” means the services provided by Accord under the Services Agreement.
- “Services Agreement” has the meaning given in the Background.
- “Sub-processor” means any processor engaged by Accord to process Personal Data on its behalf.
- “Restricted Transfer” means a transfer of Personal Data that would be prohibited by the GDPR or UK GDPR absent the appropriate safeguards referred to in this DPA.

1.2 In the event of any conflict between this DPA and the Services Agreement, this DPA prevails in relation to the subject matter of processing Personal Data. In the event of any conflict between this DPA and the EU SCCs or the UK Addendum, the EU SCCs or UK Addendum (as applicable) prevail.

## 2. Subject Matter, Duration, Nature, and Purpose

2.1 The subject matter, duration, nature, and purpose of processing, the types of Personal Data processed, and the categories of data subjects are specified in Annex I.B of this DPA. Those details are deemed incorporated into this DPA.

2.2 This DPA applies for so long as Accord processes Personal Data on behalf of the Customer under the Services Agreement.

## 3. Roles of the Parties

3.1 With respect to Personal Data processed under the Services Agreement, the Customer is the controller and Accord is the processor, each as defined in Article 4 GDPR and UK GDPR.

3.2 Each Party is responsible for its own compliance with applicable data protection laws. The Customer is responsible for establishing a lawful basis for its processing, for providing all required notices to data subjects, and for obtaining any required consents.

3.3 Relationship with Discord. The Accord platform ingests Discord Server Data via the Discord API under the Discord Developer Terms of Service, which characterises Accord as an independent controller in respect of that data for the purposes of its own contractual relationship with Discord Netherlands B.V. The Parties acknowledge that this does not affect the allocation of roles between Accord and the Customer under this DPA: as between the Parties, the Customer remains the controller and Accord remains the processor of the Discord Server Data for the purposes set out in Annex I.B. Where Accord is compelled by the Discord Developer Terms of Service to take an action in respect of Discord Server Data (for example, deletion of API Data at Discord’s direction, or suspension of API access), such action is a “permitted disclosure” or “permitted deletion” under this DPA, and Accord will notify the Customer to the extent legally permitted.

## 4. Processor Obligations

Accord shall:

- (a) process Personal Data only on documented instructions from the Customer, including the instructions set out in the Services Agreement and this DPA, unless otherwise required by applicable EU Member State, UK, or Australian law to which Accord is subject (in which case

Accord shall notify the Customer of that legal requirement before processing, unless prohibited from doing so);

- (b) ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (c) implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including at minimum the measures set out in Annex II;
- (d) assist the Customer, taking into account the nature of the processing and the information available to Accord, in fulfilling the Customer's obligations under Articles 32–36 GDPR, including by providing information as reasonably requested;
- (e) taking into account the nature of the processing, assist the Customer by appropriate technical and organisational measures, insofar as possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights under Chapter III GDPR; if a data subject makes a request directly to Accord, Accord shall promptly forward the request to the Customer;
- (f) make available to the Customer all information necessary to demonstrate compliance with this DPA and Article 28 GDPR, and allow for and contribute to audits as provided in Clause 11;
- (g) immediately inform the Customer if, in its opinion, an instruction from the Customer infringes the GDPR, UK GDPR, or other Union or Member State data protection provisions;
- (h) at the Customer's choice, delete or return all Personal Data to the Customer at the end of the provision of Services relating to processing, and delete existing copies unless Union or Member State law or Australian law requires storage of Personal Data. The default position, unless the Customer instructs otherwise in writing within 30 days after termination or expiry of the Services Agreement, is that Accord shall delete all Personal Data within 30 days and certify deletion in writing.

## 5. Sub-processors

5.1 The Customer provides general authorisation for Accord's engagement of Sub-processors listed in Annex III (and at Accord's sub-processor register at <https://accord.gg/legal/sub-processors>), subject to the requirements of this Clause 5.

5.2 Accord shall give the Customer at least 14 days' prior written notice (which may be given by email or by publication at <https://accord.gg/legal/sub-processors> for Customers subscribed to update notifications there) of any intended addition or replacement of a Sub-processor.

5.3 The Customer may object in good faith to any new Sub-processor within 14 days of such notice. If the Customer objects on reasonable data protection grounds, the Parties shall work together in good faith to resolve the objection. If no resolution is reached, the Customer may terminate the portion of the Services Agreement relating to the Services that cannot be provided without the engagement of the Sub-processor, by providing written notice. Accord shall refund any prepaid but unused fees for the affected Services. Such termination shall be without penalty to either Party.

5.4 Where Accord engages a Sub-processor, it shall do so by way of a written contract that imposes on the Sub-processor, in substance, the same data protection obligations as those binding Accord under this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures as required by Article 28(3) GDPR.

5.5 Accord remains fully liable to the Customer for the performance of each Sub-processor's obligations.

## 6. International Transfers

6.1 The Customer acknowledges that Accord is established in Australia and that its personnel, Affiliates, and Sub-processors may be located in third countries outside the EEA and the United Kingdom. Any such transfer constitutes a Restricted Transfer.

6.2 To the extent the Customer's transfer of Personal Data to Accord is a Restricted Transfer subject to the GDPR:

- (i) the Parties agree to comply with the EU SCCs (Module Two – Controller to Processor), which are incorporated into this DPA by reference and completed by Annex I, Annex II, and Annex III; and
- (j) Accord shall implement and maintain the technical, organisational, and contractual supplementary measures set out in the Transfer Impact Assessment provided to the Customer (the "TIA"), and shall co-operate with the Customer in any re-assessment thereof.

6.3 To the extent the transfer is a Restricted Transfer subject to the UK GDPR, the EU SCCs are incorporated into this DPA as amended by the UK Addendum (Annex B). Details required by the UK Addendum are set out in Annex B Part 1 Tables 1–4.

6.4 For onward transfers by Accord to Sub-processors located outside the EEA or the United Kingdom, Accord shall put in place (a) EU SCCs (and, where applicable, the UK Addendum), (b) reliance on an adequacy decision (including the EU–US Data Privacy Framework and the UK Extension to it, where applicable), or (c) another valid transfer mechanism under Articles 45–49 GDPR.

## 7. Data Subject Rights

7.1 Taking into account the nature of the processing, Accord shall assist the Customer, by appropriate technical and organisational measures and insofar as possible, to fulfil the Customer's obligation to respond to requests from data subjects exercising their rights under the GDPR and UK GDPR.

7.2 If Accord receives a request directly from a data subject, it shall not respond substantively to that request but shall promptly notify the Customer, providing reasonable information to enable the Customer to respond. This does not prevent Accord from making the acknowledgements and providing the information required by the Accord Privacy Policy, including processing verified deletion or access requests in respect of Discord User IDs as described in that policy.

## 8. Security

8.1 Accord shall implement and maintain the technical and organisational measures set out in Annex II (Technical and Organisational Measures). Accord may update those measures from time to time provided that the overall level of security is not materially reduced.

## 9. Personal Data Breaches

9.1 Accord shall notify the Customer without undue delay, and in any event within 72 hours after becoming aware of a Personal Data breach affecting Personal Data processed on behalf of the Customer.

9.2 The notification shall include, to the extent known at the time: (a) a description of the nature of the breach, including where possible the categories and approximate numbers of data subjects and Personal Data records affected; (b) the name and contact details of Accord's contact point; (c) a

description of the likely consequences; and (d) a description of the measures taken or proposed to address the breach and to mitigate its effects.

9.3 Where the information required cannot be provided at the same time, the information may be provided in phases without further undue delay.

## **10. Data Protection Impact Assessments and Consultation**

10.1 Accord shall provide reasonable assistance to the Customer in carrying out data protection impact assessments and in consulting supervisory authorities as required under Articles 35 and 36 GDPR, taking into account the nature of processing and the information available to Accord.

## **11. Audits**

11.1 Accord shall make available to the Customer, on reasonable written request and at reasonable intervals (no more than once in any 12-month period, except where legally required or following a confirmed Personal Data breach), all information necessary to demonstrate compliance with this DPA and Article 28 GDPR.

11.2 The Customer (or an independent third-party auditor mandated by the Customer and reasonably acceptable to Accord, bound by appropriate confidentiality obligations) may, at the Customer's cost and on at least 30 days' prior written notice, conduct an audit of Accord's processing activities under this DPA. Audits shall be conducted during normal business hours, in a manner that does not materially disrupt Accord's operations, and subject to Accord's reasonable on-site policies.

11.3 Accord may satisfy its obligations under this Clause 11 by providing, in the first instance, an up-to-date written response to a reasonable set of security and compliance questions and, where available, copies of any third-party certifications, audit reports, or penetration test summaries it has obtained.

## **12. Termination and Return or Deletion of Personal Data**

12.1 On termination or expiry of the Services Agreement, Accord shall, in accordance with Clause 4(h), delete all Personal Data processed on behalf of the Customer within 30 days and certify deletion in writing, unless the Customer instructs Accord in writing within 30 days after termination or expiry to return the Personal Data prior to deletion. The default position is deletion without return.

12.2 Accord may retain Personal Data to the extent required by EU, UK, Member State, or Australian law, or in the form of strictly anonymised and aggregated data that cannot be used to identify any individual and that is therefore not Personal Data.

## **13. Liability**

13.1 Each Party's aggregate liability arising out of or in connection with this DPA, whether in contract, tort (including negligence), for breach of statutory duty, or otherwise, is subject to the liability provisions in the Services Agreement, including any aggregate cap on liability.

13.2 Notwithstanding Clause 13.1, and solely for the purpose of allocating liability between the Parties, the Parties agree that in no event shall either Party's aggregate liability under this DPA exceed the total fees paid by the Customer to Accord under the Services Agreement in the 12 months immediately preceding the event giving rise to the claim. This cap does not apply to (a)

Accord’s indemnification obligations expressly agreed in the Services Agreement, (b) either Party’s liability for fraud or wilful misconduct, or (c) any liability which cannot be limited or excluded by law.

13.3 For the avoidance of doubt, nothing in this Clause 13 limits a data subject’s third-party beneficiary rights under Clause 3 of the EU SCCs, Accord’s or the Customer’s liability to a data subject under Clause 12 of the EU SCCs, or the Parties’ respective liabilities to each other under Clause 12(d) and (f) of the EU SCCs. Any compensation paid by one Party to a data subject in respect of a breach of third-party beneficiary rights caused by the other Party (or its Sub-processor) may be recovered from that other Party in accordance with Clause 12 of the EU SCCs.

## 14. Order of Precedence

In the event of conflict, the following order of precedence applies: (a) the EU SCCs and, where applicable, the UK Addendum; (b) this DPA; (c) the Services Agreement.

## 15. Governing Law and Jurisdiction

15.1 This DPA, other than the EU SCCs and the UK Addendum, is 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 relation to any dispute arising out of or in connection with this DPA.

15.2 The EU SCCs are governed by the law of Ireland in accordance with Clause 17 of the EU SCCs, and disputes arising out of or in connection with the EU SCCs shall be resolved by the courts of Ireland in accordance with Clause 18 of the EU SCCs. The UK Addendum is governed by the laws of England and Wales.

15.3 Nothing in this Clause 15 restricts a data subject’s ability to bring proceedings in the courts of the Member State of habitual residence, as provided in Clause 18(c) of the EU SCCs.

## 16. Acceptance and Signatures

16.1 This DPA is accepted by the Customer on the earlier of: (a) the Customer’s execution of the Services Agreement, where that Agreement incorporates this DPA by reference; or (b) the Customer’s written or electronic assent to this DPA.

16.2 The Customer may request a signed counterpart of this DPA from [privacy@accord.gg](mailto:privacy@accord.gg). The counterpart uses the Customer-specific details set out in the Services Agreement to complete the signature block below and the Annex I “List of Parties”. Execution of a counterpart does not vary the substantive terms of this DPA.

| For ACCORD DATA PTY LTD                                     | For the CUSTOMER            |
|---|-----------------------------|
| Signature: _____  | Signature: _____            |
| Name: Christopher Illuk                                     | Name: _____                 |
| Title: Director   | Title: _____                |
| Email: <a href="mailto:chris@accord.gg">chris@accord.gg</a> | Email: _____                |
| Date: _____   | Legal entity name:<br>_____ |

|  |   |
|--|---|
|  | <p>Registration number:<br/>_____</p> <p>Registered address:<br/>_____</p> <p>Date: _____</p> |
|--|---|

## ANNEX A — EU STANDARD CONTRACTUAL CLAUSES (MODULE TWO): APPENDIX

The Parties agree to the EU Standard Contractual Clauses, Module Two (Transfer controller to processor), as set out in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, the full text of which is incorporated into this DPA by reference. The Appendix to those Clauses is completed as follows.

Optional Clauses, Module selections, and completion of variable fields:

- Clause 7 (Docking clause) is not adopted.
- Clause 9(a): Option 2 (general written authorisation) applies; prior-notification period is 14 days.
- Clause 11(a): the optional redress clause (independent dispute resolution body) is not adopted.
- Clause 17: Option 1; these Clauses are governed by the law of Ireland.
- Clause 18(b): any dispute is resolved by the courts of Ireland.

### Annex I.A — List of Parties

#### Data Exporter (Controller)

|  |   |
|--|---|
| <b>Name</b>                            | The Customer, as identified in the Services Agreement.  |
| <b>Registration number</b>             | As set out in the Services Agreement.   |
| <b>Address</b>                         | As set out in the Services Agreement.   |
| <b>Contact person</b>                  | The Customer's data-protection or authorised contact, as identified in the Services Agreement or subsequent written notice to Accord. |
| <b>Activities relevant to transfer</b> | Receipt of Services under the Services Agreement; designation of Discord communities for analysis through the Accord platform.        |
| <b>Role</b>                            | Controller  |

#### Data Importer (Processor)

|  |   |
|--|---|
| <b>Name</b>                                | ACCORD DATA PTY LTD   |
| <b>Registration numbers</b>                | ACN 691 164 584; ABN 60 691 164 584   |
| <b>Address</b>                             | Suite 3, 99 Musgrave Road, Red Hill QLD 4059, Australia   |
| <b>Contact person</b>                      | Christopher Illuk, Director — <a href="mailto:chris@accord.gg">chris@accord.gg</a> (privacy queries: <a href="mailto:privacy@accord.gg">privacy@accord.gg</a> )                                       |
| <b>EU representative (Article 27 GDPR)</b> | Prighter Group, as Accord's appointed EU representative for EU data subjects. Contact portal: <a href="https://app.prighter.com/portal/16232110925">https://app.prighter.com/portal/16232110925</a> . |
| <b>Activities relevant to transfer</b>     | Provision of the Accord platform and services; remote access and processing of Personal Data transferred from the EEA/UK.   |
| <b>Role</b>                                | Processor   |

### Annex I.B — Description of Transfer

### **Categories of data subjects**

- Personnel, representatives, and end-users of the Customer who use the Accord platform (“Platform Users”).
- End-users of Discord servers and public Discord channels designated by the Customer for analysis through the Accord platform (“Discord Users”), typically members of public Discord communities operated by or relevant to the Customer.

### **Categories of personal data**

Platform Data (relating to Platform Users):

- Identifiers: name or organisation name; email address; account username.
- Authentication data: hashed credentials and session data held by the identity provider; single-sign-on identifiers.
- Transactional data: subscription or purchase records (where applicable).
- Communications with Accord (support and feedback).
- Usage and telemetry data about use of the Services.

Discord Server Data (relating to Discord Users, processed on documented instructions of the Customer):

- Textual content of messages posted in public Discord channels designated by the Customer.
- Discord User IDs (unique 18-digit identifier).
- Discord username at the time of collection.
- Associated metadata: timestamps, server IDs, channel IDs, roles (where public).

### **Sensitive data**

No special categories of personal data (Article 9 GDPR) or data relating to criminal convictions and offences (Article 10 GDPR) are intentionally processed. Because Discord Server Data consists of messages voluntarily posted by Discord Users in public channels, such messages may incidentally contain content that discloses data falling within those categories. The safeguards applied are: strict purpose limitation; access controls on Accord’s personnel (see Annex II); logging of privileged access; and the processing instructions that Discord Server Data is not analysed for special-category attributes.

### **Frequency of the transfer**

Continuous, for as long as the Services Agreement is in force and the Customer designates Discord communities for analysis.

### **Nature of the processing**

- Collection of Discord Server Data from public Discord channels via the Discord API.
- Storage, organisation, analysis, classification, summarisation (including via large language model inference), and retrieval of such data.
- Delivery of insights, analytics, and reports to the Customer through the Accord platform.
- Operation and administration of the Customer’s Accord account; provision of support; service monitoring.

### **Purpose(s) of the data transfer and further processing**

- To provide the Customer with insights and analytics in respect of community activity in the Discord servers it designates.
- To manage and maintain the Customer’s Accord account and provide customer support.
- To monitor, secure, and improve the Accord platform.
- For strictly anonymised and aggregated analysis that does not identify any natural person.

## Retention

- Platform Data: retained for the duration of the Services Agreement and for up to 6 years after termination for legal, tax, and accounting purposes, unless earlier deletion is requested and permitted.
- Discord Server Data: retained for so long as the Customer maintains the relevant designation and the Services Agreement is in force. Customer-specific Discord Server Data is deleted from active systems within 30 days of termination, in accordance with Clause 12 of this DPA.
- Anonymised and aggregated data: may be retained indefinitely as non-personal data.

## Sub-processors

Subject matter, nature, and duration of processing are as set out in Annex III and in the Accord sub-processor register at <https://accord.gg/legal/sub-processors>.

## Annex I.C — Competent Supervisory Authority

The competent supervisory authority of the data exporter is determined in accordance with Clause 13 of the EU SCCs, by reference to the Customer's place of establishment or, where the Customer is not established in an EU Member State, the location of the data subjects most affected by the processing. Where the Customer is established in an EU Member State, the competent supervisory authority is the data protection authority of that Member State. Where the Customer is established outside the EU but processes personal data of data subjects in the EU, the competent supervisory authority is determined under Clause 13(a)(ii) of the EU SCCs.

Where the Customer wishes to record a specific supervisory authority for the purposes of Annex I.C, it shall do so by notice to Accord at [privacy@accord.gg](mailto:privacy@accord.gg), and Accord will countersign a counterpart of this DPA that records the specific supervisory authority identified. Absent such notice, the default rule in the preceding paragraph applies.

## **ANNEX II — Technical and Organisational Measures (TOMs)**

Description of the technical and organisational measures implemented by Accord to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of processing and the risks for the rights and freedoms of natural persons.

### **Measures of pseudonymisation and encryption of personal data; measures for the protection of data during transmission**

Communication and transport control. Measures to ensure that data cannot be read, copied, modified, or deleted without authorisation during electronic transmission, including:

- Transport encryption via HTTPS/TLS.
- Session management with TTL and logout functions.
- Network segmentation and firewall protection.
- Internal separation of access to infrastructure and management of SSH access.
- Secure Shell (SSH) with key-based authentication.
- Traffic and service monitoring by a dedicated operations team.

### **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services; restoration of availability in the event of a physical or technical incident**

Availability control. Measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical), including:

- Distributed high-availability service architecture.
- Backup procedures.
- Mirroring of disks (e.g., RAID technology) at the infrastructure provider level.
- Uninterruptible power supply (UPS) at the data-centre provider level.
- Remote storage.

### **Measures for user identification and authorisation**

Access restriction mechanisms. Measures to prevent unauthorised use of data-processing systems, including:

- Multi-layered network/systems access restriction architecture.
- User identification and authentication procedures.
- Strong credential policy (complexity, minimum length, rotation).
- Two-factor authentication.
- Automatic blocking (e.g., password lock-out or session timeout).
- Monitoring of authentication failures and automatic account lock after repeated erroneous attempts.

### **Measures for the protection of data during storage**

Data access control. Measures to ensure that authorised users gain access only to Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified, or deleted without authorisation, including:

- Internal logical access-control policies and procedures.

- Authorisation schemes and role-based permissions.
- Differentiated access rights via roles and permissions.
- Logging of accesses.
- Limiting and monitoring of privileged access.
- Access reports and centralised procedures for granting, revoking, and regularly reviewing access.

### **Measures for ensuring physical security of processing locations**

Physical access control (implemented at the infrastructure-provider level):

- Defined security areas with restricted access (data centres, server rooms).
- Access authorisations for employees and third parties, and visitor registration.
- Access control systems (e.g., magnetic cards).
- Door locking (electric door openers, etc.).
- Security staff.
- Surveillance, video/CCTV monitoring, and alarm systems.

### **Measures for ensuring events logging**

Entry control. Measures to monitor whether data have been entered, changed, or removed from data-processing systems, via logging and reporting capabilities.

### **Measures for ensuring system configuration, including default configuration**

Change management controls with appropriate validation and approvals. Deployment of changes under the control of configuration-management systems.

### **Measures for internal IT and IT security governance and management; certification / assurance**

Accord maintains written internal information-security policies, assigns ownership of security controls, and periodically reviews those controls. Accord does not presently hold third-party security certifications (e.g., ISO 27001 or SOC 2); it will update Annex II if and when such certifications are obtained.

### **Measures for ensuring data minimisation**

A risk-based approach is used to determine the minimum amount of data to be processed, applied during data-protection impact assessments and in the design of the Services.

### **Measures for ensuring data quality; data portability and erasure**

Quality, portability, and erasure are supported via self-service tools and dedicated support procedures within the Accord platform. Verified deletion requests are handled in accordance with the Accord Privacy Policy and the Accord Data Access Request Policy.

### **Measures for ensuring limited data retention**

Application of the retention periods set out in Annex I.B and in the Accord Privacy Policy.

### **Measures for ensuring accountability**

Processing control. Measures to ensure that data are processed solely in accordance with the Customer's instructions, including:

- Clear and detailed wording of the Services Agreement and this DPA.
- Obligations of confidentiality imposed on personnel and Sub-processors.
- Confidentiality agreements/clauses with employees and (sub)contractors.

### **Measures for sub-processor assistance**

Accord contracts with Sub-processors on terms that require them to implement technical and organisational measures at least equivalent in substance to those set out above, and to assist Accord (and, through Accord, the Customer) in meeting the Customer's obligations under Articles 32–36 GDPR and Articles 12–22 GDPR.

## ANNEX III — List of Sub-processors

The Customer provides general written authorisation for the engagement of the following Sub-processors. This Annex is maintained current and is mirrored at <https://accord.gg/legal/sub-processors>, which is the authoritative record; changes are notified under Clause 5 of this DPA.

| Sub-processor   | Legal entity   | Country      | Processing activity   | Hosting region                                 | Transfer mechanism  |
|---|--|--------------|---|--|---|
| Auth0   | Okta, Inc.   | USA          | Identity, authentication, and session management for the Accord platform  | US (Auth0 US region)                           | EU SCCs / EU-US DPF   |
| Google Cloud Platform — Database hosting                              | Google Ireland Limited (operating as GCP) / Google LLC | Ireland (EU) | Primary application database (managed Postgres) and associated storage  | europa-west / EU region                        | Intra-EEA (no transfer mechanism required for this service component) |
| Google Vertex AI  | Google LLC   | USA          | Large language model inference for analysis, classification, and summarisation of Discord Server Data   | us-central1                                    | EU SCCs / EU-US DPF   |
| Vercel (hosting, AI Gateway, Blob Storage, Analytics, Speed Insights) | Vercel Inc.  | USA          | Hosting of the Accord web application, AI request routing, static/blob storage for uploaded assets, web analytics, and performance monitoring | US (with EU blob region used where configured) | EU SCCs / EU-US DPF   |
| Upstash Redis   | Upstash, Inc.  | USA          | In-memory cache for session and metadata acceleration   | US (default)                                   | EU SCCs / EU-US DPF   |
| Resend  | Resend, Inc.   | USA          | Transactional email (account invites, notifications)  | US   | EU SCCs / EU-US DPF   |
| HubSpot   | HubSpot, Inc.  | USA          | Customer relationship management and marketing-site forms (sign-up, newsletter) — Platform Data only  | US   | EU SCCs / EU-US DPF   |

| Sub-processor  | Legal entity                      | Country   | Processing activity   | Hosting region        | Transfer mechanism   |
|----------------|-----------------------------------|---|---|-----------------------|--|
| PostHog        | PostHog Inc. (EU-hosted instance) | United Kingdom / EU region                          | Product analytics and monitoring of the Accord platform                               | eu.i.posthog.com (EU) | UK IDTA / EU SCCs as required; EU-hosted service           |
| Knock          | Knock Labs, Inc.                  | USA   | Notification orchestration (email/in-app) for Platform Users                          | US                    | EU SCCs / EU-US DPF  |
| Temporal Cloud | Temporal Technologies, Inc.       | USA (service operated via Temporal Cloud EU region) | Workflow orchestration for data ingestion and analytics pipelines on Accord's backend | EU region             | EU SCCs / EU-US DPF (as applicable to the Temporal entity) |

Notes:

- “EU-US DPF” refers to the EU-U.S. Data Privacy Framework and the UK Extension to it, adopted by the European Commission’s adequacy decision of 10 July 2023, insofar as the recipient entity is certified under it. Where certification does not cover the transfer, the EU SCCs apply.
- Subject matter, nature, and duration of processing: same as the primary processing described in Annex I.B, limited to the activities described for each Sub-processor above, for the duration of the Services Agreement.

## ANNEX B — UK INTERNATIONAL DATA TRANSFER ADDENDUM (Part 1 Tables)

This Addendum incorporates the template published by the UK Information Commissioner’s Office, in the form of the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0, in force 21 March 2022) (the “UK Addendum”). The UK Addendum is incorporated by reference. Its Mandatory Clauses apply with Part 1 of the Addendum completed as set out below.

**Table 1 — Parties**

|   |  |   |
|---|--|---|
| <b>Start date</b>                                 | The date this DPA takes effect in accordance with Clause 16.1.                                 |   |
| <b>The Parties</b>                                | <b>Exporter (Controller)</b>   | <b>Importer (Processor)</b>   |
| <b>Parties’ details</b>                           | The Customer, as identified in the Services Agreement.   | ACCORD DATA PTY LTD (ACN 691 164 584; ABN 60 691 164 584), Suite 3, 99 Musgrave Road, Red Hill QLD 4059, Australia. |
| <b>Key Contact</b>                                | The Customer’s data-protection or authorised contact, as identified in the Services Agreement. | Christopher Illuk, Director — chris@accord.gg / privacy@accord.gg   |
| <b>Signature (if required for the Start Date)</b> | As per Clause 16 of the DPA.   | As per Clause 16 of the DPA.  |

**Table 2 — Selected SCCs, Modules and Selected Clauses**

|  |   |
|--|---|
| <b>Addendum EU SCCs</b>                                | The Approved EU SCCs in force under Commission Implementing Decision (EU) 2021/914 of 4 June 2021, attached to this DPA as Annex A, Module Two (Controller to Processor). |
| <b>Module in operation</b>                             | Module Two.   |
| <b>Clause 7 (Docking clause)</b>                       | Not adopted.  |
| <b>Clause 11 (Option)</b>                              | Independent dispute-resolution body not adopted.  |
| <b>Clause 9(a) — Prior authorisation</b>               | General written authorisation — 14 days’ prior notice of changes.   |
| <b>Clause 17 — Governing law</b>                       | Law of Ireland.   |
| <b>Clause 18(b) — Choice of forum and jurisdiction</b> | Courts of Ireland.  |

**Table 3 — Appendix Information**

The “Appendix Information” referenced in Table 3 of the UK Addendum is as set out in this DPA:

- Annex 1A (List of Parties): see Annex A, Annex I.A of this DPA.
- Annex 1B (Description of Transfer): see Annex A, Annex I.B of this DPA.

- Annex II (Technical and Organisational Measures): see Annex II of this DPA.
- Annex III (List of Sub-processors): see Annex III of this DPA.

**Table 4 — Ending this Addendum when the Approved Addendum Changes**

Which Parties may end this Addendum as set out in Section 19: Neither Party.

## Change log

The most recent version of this DPA is published at <https://accord.gg/legal/dpa>. Material changes are notified to active Customers in accordance with the terms set out under “How this DPA takes effect”.

| Version | Date          | Change summary   |
|---------|---------------|--|
| 1.0     | 24 April 2026 | Initial publication at <a href="https://accord.gg/legal/dpa">accord.gg/legal/dpa</a> . |

— — END OF DOCUMENT — —