DATA PROCESSING AGREEMENT

This data processing agreement is between Corrily, Inc. (the "**Data Processor**") and the Data Controller(s) (as defined below) and incorporates the terms and conditions set out in the Schedules hereto (the "**Agreement**").

Each Data Controller has appointed Data Processor to provide services to the Data Controller(s). As a result of its providing such services to the Data Controller(s), Data Processor will store and process certain personal information of the Data Controller(s), in each case as described in further detail in Schedule 2 (*Processing Details*).

The Agreement is being put in place to ensure that Data Processor processes each Data Controller's personal data on the Data Controller's instructions and in compliance with Applicable Data Protection Laws.

The parties to this Agreement hereby agree to be bound by the terms and conditions in the attached Schedules as applicable with effect from the date of this Agreement (the "**Effective Date**").

This Agreement may be executed in any number of counterparts, each of which is an original and all of which evidence the same agreement between the parties.

Accepted and agreed to by:

Signature: _____

Name: _____

On behalf of: Corrily, Inc. 2261 Market Street 4154
San Francisco, CA 94114

(the "**Data Processor**")

and by:

Signature: _____

Name: _____

Date: _____

On behalf of:

(the "**Data Controller**")

Schedule 1
STANDARD TERMS FOR PROCESSING AGREEMENT

BACKGROUND:

(a) Each Data Controller wishes to appoint Data Processor to Process Personal Data, as further described in Schedule 2 (*Processing Details*).

(b) The Agreement is being put in place to ensure that Data Processor processes each Data Controller's Personal Data on Data Controller's instructions and in compliance with the Applicable Data Protection Laws (as defined below).

1. Definitions

1.1 For the purposes of this Agreement, the following expressions bear the following meanings unless the context otherwise requires:

1. "**Applicable Data Protection Laws**" means (a) Applicable European Data Protection Laws, (b) the California Consumer Privacy Act ("**CCPA**") and (c) any relevant law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or the use of personal data; in each case as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time;

2. "**Applicable European Data Protection Laws**" means (a) the General Data Protection Regulation 2016/679 (the "**GDPR**"); (b) the Privacy and Electronic Communications Directive 2002/58/EC; (c) the UK Data Protection Act 2018 ("**DPA**"), the UK General Data Protection Regulation as defined by the DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (together with the DPA, the "**UK GDPR**"), and the Privacy and Electronic Communications Regulations 2003; and (d) any relevant law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or the use of personal data in any European member state or the United Kingdom, in each case as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time;

"**Controller to Processor Clauses**" means (i) in respect of transfers of Personal Data subject to the GDPR, the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021, specifically including Module 2 (Controller to Processor); and (ii) in respect of transfers of Personal Data subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner, in each case as amended, updated or replaced from time to time;

"**Data Subject**" shall have the meaning given in the relevant Applicable Data Protection Laws;

"**Personal Data**" shall have the meaning given in the relevant Applicable Data Protection Laws;

"**Process**", "**Processed**" or "**Processing**" shall have the meaning given in the relevant Applicable Data Protection Laws;

"**Processor to Processor Clauses**" means, as relevant, (i) in respect of transfers of Personal Data subject to the GDPR, the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021 specifically including Module 3 (Processor to Processor); (ii) in respect of transfers of Personal Data subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner, in each case as amended, updated or replaced from time to time;

"**Regulator**" means a data protection supervisory authority which has jurisdiction over a Data Controller's Processing of Personal Data; and

"**Third Country**" means (i) in relation to Personal Data transfers subject to the GDPR, any country outside of the scope of the data protection laws of the European Economic Area, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time; and (ii) in relation to Personal Data transfers subject to the UK GDPR, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing adequate protection for Personal Data by the relevant competent authority of the UK from time to time.

2. Conditions of Processing

2.1 This Agreement governs the terms under which Data Processor is required to Process Personal Data on behalf of the Data Controller(s). Clause 4 applies only to the extent that the Data Controller(s) is a "business" and shares with Data Processor Personal Data in a manner which would otherwise constitute a "sale", as those terms are defined by the CCPA. Clauses 5, 6 and 7 apply only to the extent that Data Processor's Processing of Personal Data is subject to Applicable European Data Protection Laws.

3. Changes in Applicable Data Protection Laws

3.1 The parties agree to negotiate in good faith modifications to this Agreement if changes are required for Data Processor to continue to process the Personal Data as contemplated by this Agreement in compliance with the Applicable Data Protection Laws or to address the legal interpretation of the Applicable Data Protection Laws, including (i) to comply with the GDPR or any national legislation implementing it, the UK General Data Protection Regulation, the DPA or the CCPA, and any guidance on the interpretation of any of their respective provisions; (ii) the Controller to Processor Clauses or the Processor to Processor Clauses or any other mechanisms or findings of adequacy are invalidated or amended, or (iii) if changes to the membership status of a country in the European Union or the European Economic Area require such modification.

4. Data Processor's Obligations under the CCPA

4.1 Data Processor will Process Personal Data as a service provider on the Data Controller(s) behalf for one or more business purposes as set forth in the Agreement and in Schedule 2 (*Processing Details*), or as otherwise permitted by the CCPA. Data Processor shall not retain, use or disclose such Personal Data other than for those purposes, including retaining, using or disclosing such Personal Data for a commercial purpose other than performing the services.

4.2 The parties agree that the existence of this Agreement does not constitute an admission that sharing of Personal Data constitutes a sale.

4.3 The terms "business purpose" "commercial purpose", "sale" and "service provider" in this section have the meanings set forth in the CCPA.

5. Data Processor's Obligations under Applicable European Data Protection Laws

5.1 Data Processor shall only Process Personal Data on behalf of the Data Controller(s) and in accordance with, and for the purposes set out in the documented instructions received from the Data Controller(s) unless required to Process such Personal Data by applicable law to which the Data Processor is subject; in such a case, the Data Processor shall inform the Data Controller(s) of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

5.2 Data Processor shall ensure that its personnel authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.3 Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of the Processing as set out in Schedule 3, or otherwise agreed and documented between the Data Controller and Data Processor from time to time.

5.4 Data Processor shall without undue delay notify the relevant Data Controller(s) about any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Personal Data belonging to the Data Controller(s) or any accidental or unauthorised access or any other event affecting the integrity, availability or confidentiality of the Personal Data belonging to the Data Controller(s).

5.5 Data Processor shall upon written request from any Data Controller from time to time provide that Data Controller with such information as is reasonably necessary to demonstrate compliance with the obligations laid down in this Agreement.

5.6 Data Processor shall permit each Data Controller at any time upon seven (7) days' notice, to be given in writing, to have access to the appropriate part of Data Processor's premises, systems, equipment, and other materials and data Processing facilities to enable the relevant Data Controller to inspect or audit the same for the purposes of monitoring compliance with Data Processor's obligations under this Agreement. Such inspection shall:

(i) be carried out by any Data Controller or an inspection body composed of independent members and in possession of the required professional qualifications and bound by a duty of confidentiality, selected by the Data Controller(s), where applicable, in agreement with the Regulator; and

(ii) not relieve Data Processor of any of its obligations under this Agreement.

(iii) Where:

(A) a Data Subject exercises his or her rights under the Applicable European Data Protection Law in respect of Personal Data Processed by Data Processor on behalf of any Data Controller, including Data Subjects exercising rights under Applicable European Data Protection Laws (such as rights to rectification, erasure, blocking, access their personal data, objection, restriction of processing, data portability, and the right not to be subject to automated decision making); or

(B) any Data Controller is required to deal or comply with any assessment, enquiry, notice or investigation by the Regulator; or

(C) any Data Controller is required under the Applicable European Data Protection Laws to carry out a mandatory data protection impact assessment or consult with the Regulator prior to Processing Personal Data entrusted to the Data Processer under this Agreement,

then Data Processor will provide reasonable assistance to the relevant Data Controller to enable that Data Controller to comply with obligations which arise as a result thereof.

5.7 To the extent the Data Processor Processes Personal Data in a Third Country, and it is acting as data importer, the Data Processor shall, comply with the data importer's obligations set out in the Controller to Processor Clauses, which are hereby incorporated into and form part of this Agreement; the Data Controller(s) will comply with the data exporter's obligations in such Controller to Processor Clauses; and:

(i) if applicable, for the purposes of Part 1 of such Controller to Processor Clauses, the relevant Addendum EU SCCs (as such term is defined in the applicable Controller to Processor Clauses) are the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021 (Module 2) as incorporated into this Agreement;

(ii) for the purposes of Annex I or Part 1 (as relevant) of such Controller to Processor Clauses, the parties and processing details set out in Schedule 2 (*Processing Details*) shall apply, and the Start Date is the Effective Date;

(iii) for the purposes of Annex II of such Controller to Processor Clauses, [the technical and organisational security measures set out in Schedule 3 (*Technical and Organisation Security Measures*) shall apply; and

(iv) if applicable, for the purposes of: (i) Clause 9 of such Controller to Processor Clauses, Option 1 ("Specific prior authorisation") is deemed to be selected and a notice period of 30 days shall apply; (ii) Clause 11(a) of such Controller to Processor Clauses, the optional wording in relation to independent dispute resolution is deemed to be included; (iii) Clause 13 and Annex I.C, the competent supervisory authority shall be the EU Member State where the Data Controller is located (or the UK as applicable); (iv) Clause 17, Option 1 is deemed to be selected and the governing law shall be the EU Member State where the Data Controller is located (or the UK as applicable); (v) Clause 18, the competent courts shall be the EU Member State where the Data Controller is located (or the UK as applicable); (vi) Part 1 of such Controller to Processor Clauses, either party may terminate the Controller to Processor Clauses pursuant to Section 19 of such Controller to Processor Clauses.

5.8 The Data Controller acknowledges and agrees that Data Processor may appoint an affiliate or third party subcontractor to Process the Data Controller's Personal Data in a Third Country, in which case:

(i) the Data Processor shall execute the Processor to Processor Clauses, if applicable and available, with any relevant subcontractor (including affiliates) it appoints on behalf of the Data Controller; or

(ii) the Data Controller grants Data Processor a mandate to execute the relevant Controller to Processor Clauses (with the processing details set out in Schedule 2 (*Processing Details*) and the technical and organisational security measures set out in Schedule 3 (*Technical and Organisation Security Measures*) applying for the purposes of Appendix 1 and Appendix 2, respectively)

6. Sub-Contracting

6.1 The Data Controller(s) hereby grants the Data Processor general written authorisation to engage the sub-processors set out in Schedule 4 (*Authorised Subcontractors*) for the purposes further described in Schedule 4 (*Authorised Subcontractors*), and subject to this clause 6.

6.2 If Data Processor appoints a new Subcontractor or intends to make any changes concerning the addition or replacement of the Subcontractors set out in Schedule 4 (*Authorised Subcontractors*), it shall provide the Data Controller(s) with twenty 20 business days' prior written notice, during which the Data Controller(s) can object against the appointment or replacement. If no Data Controller objects, Data Processor may proceed with the appointment or replacement. The Data Processor shall ensure that it has a written agreement in place with all Subcontractors which contains obligations on the Subcontractor which are no less onerous on the relevant Subcontractor than the obligations on Data Processor under this Agreement.

7. Data Controller's Obligations

7.1 Each Data Controller warrants that: (i) the legislation applicable to it does not prevent Data Processor from fulfilling the instructions received from the Data Controller(s) and performing Data Processor's obligations under this Agreement; and (ii) it has complied and continues to comply with the Applicable Data Protection Laws, in particular that it has obtained any necessary consents or given any necessary notices, and otherwise has a legitimate ground to disclose the data to Data Processor and enable the Processing of the Personal Data by the Data Processor as set out in this Agreement and as envisaged by any services agreement in place between the parties.

7.2 Each Data Controller agrees that it will jointly and severally together with any other Data Controller, indemnify and hold harmless Data Processor on demand from and against all claims, liabilities, costs, expenses, loss or damage (including consequential losses, loss of profit and loss of reputation and all interest, penalties and legal and other professional costs and expenses) incurred by Data Processor arising directly or indirectly from a breach of this Clause 7.

8. Termination

8.1 Termination of this Agreement shall be governed by section 9 of the Terms of Service..

9. Consequences of Termination

9.1 Upon termination of this Agreement in accordance with Clause 8 (*Termination*), the Data Processor shall, at the choice of the Data Controller:

(i) return to the Data Controller all of the Personal Data and any copies thereof which it is Processing or has Processed upon behalf of that Data Controller; or

(ii) destroy all Personal Data it has Processed on behalf of the Data Controller after the end of the provision of services relating to the Processing, and destroy all copies of the Personal Data unless any European Member State law requires storage of such Personal Data; and

(iii) in each case cease Processing Personal Data on behalf of the Data Controller(s).

10. Law and Jurisdiction

This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in all respects in accordance with the laws of California and shall be deemed to have been made in California , and each party hereby submits to the jurisdiction of the courts of San Francisco, California.

Schedule 2

PROCESSING DETAILS

A. LIST OF PARTIES

Data exporter(s):

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Role (controller/processor): Controller

Data importer(s): Corrily Inc.

1. Name: Corrily Inc.

Address:2261 Market Street 4154, San Francisco, CA 94114
Contact person's name, position and contact details: Andrej Zukov Gregoric, CTO at Corrily Inc., Phone number +447976097969, email: andrej@corrily.com

Activities relevant to the data transferred under these Clauses: Processing in order to provide services to the Controller's end users.

Role (controller/processor): Processor

GDPR Representatives of the Processor (Corrily Inc.)

1. Name: GDPR Local Ltd.
Address: GDPR Local Ltd 1st Floor Front Suite 27-29 North Street, Brighton England BN1 1EB
Contact person's name, position, and contact details: Adam Brogden, UK Representative, Phone number: +441 772 217 800; email: contact@gdprlocal.com

Activities relevant to the data transferred under these Clauses: Processing in order to represent the Processor in the UK in case of GDPR requests

Role: Representative of the Processor in the UK

2. Name: Instant EU GDPR Representative Ltd
Address: INSTANT EU GDPR REPRESENTATIVE LIMITED Office 2 12A Lower Main Street, Lucan Co. Dublin K78 X5P8 Ireland
Contact person's name, position, and contact details: Adam Brogden, EU Representative, Phone number: + 353 15 549 700; email: contact@gdprlocal.com

Activities relevant to the data transferred under these Clauses: Processing in order to represent the Processor in the EU in case of GDPR requests

Role: Representative of the Processor in the EU

B. PROCESSING DETAILS/ DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Employees, contractors, partners and/or customers of data exporter.

- Visitors to platforms data exporter is present on.

Categories of personal data transferred

The data transferred is the Personal Data provided by the data exporter (Client) to the data importer (Corrily) in connection with its use of Corrily's price and coupon optimization API, dashboard, and payment gateway integrations.

Such Personal Data may include, depending on the Customer's seat holder's input/interaction:

Services (As applicable)	**Categories of Personal Data**
Dashboard	**- User login and product usage data** **- User IP address and device/browser characteristics** **- User information (may include name, email address, title)**
API	**- End-user IP (if passed)** - End-user custom features (if passed)
Payment Gateway / Subscription management service Integration	**In the case of a webhook or OAuth integration and depending on the payment gateway / subscription management service, end-user:** - full-name - email address - billing address

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

End-user Personal Data passed by the data exporter (Client) through Corrily's API may include special categories of personal data (as defined in the GDPR). This may include, for example: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The restrictions and safeguards specified in Schedule 3 apply to these categories of Customer Personal Data (if any).

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous for the duration set out in the terms of service between the parties.

Nature of the processing

Collection, organization, structuring, use, storage, combination, making available on Corrily properties to provide and monitor Services outlined in the Terms in accordance with the Agreement.

Purpose(s) of the data transfer and further processing

- Provide, maintain, and improve services (in accordance with the Agreement) to the data exporter,
- Provide customer support to the data exporter,
- Otherwise fulfil Corrily's (and, if applicable, its affiliate's) obligations under its respective services agreement with the data exporter; and
- Compliance with applicable law.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of the Agreement until deletion in accordance with the provisions of the Data Processing Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As above.

Schedule 3

1 TECHNICAL AND ORGANISATION SECURITY MEASURES

1. 1. General Security Measures

Data Importer will comply with industry standard security measures (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, and incident response measures necessary to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Data Exporter's Personal Data provided by Data Exporter to Data Importer).

2. Contact Information

Data Importer's security team can be reached at security@corrily.com for any security issues or questions related to the product.

3. Compliance

Data Importer complies with the standards and practices set forth at the following web address: https://corrily.com/security. Data Exporter must contact their Corrily account manager for any additional information on the security certifications listed at the web address.

4. Information Security Program

The objective of Corrily's Information Security Program is to maintain the confidentiality, integrity and availability of its computer and data communication systems while meeting necessary legislative, industry, and contractual requirements. Data Importer shall establish, implement, and maintain an information security program that includes technical and organizational security and physical measures as well as policies and procedures to protect Data Exporter data processed by Data Importer against accidental loss; destruction or alteration; unauthorized disclosure or access; or unlawful destruction.

4.1 Access Controls

4.1.1 Access Procedures.

The Data Importer maintains formal access procedures for allowing its personnel access to the production service and components involved in building the production service. Only authorized employees are allowed access to these restricted components and all access is approved by an employee's manager and service owner. Only a small number of individuals are approved to access the restricted components. Audit records are maintained to indicate who has access to restricted components.

4.1.2 Access Mechanisms.

Access to the Data Importer's production service and build infrastructure occurs only over a secured channel and requires two-factor authentication.

4.1.3 Logging.

Access to the Data Importer's production service and build infrastructure is done using unique IDs and is logged.

4.2 Secure Software Development

Data Importer shall maintain policies and procedures to ensure that system, device, application and infrastructure development is performed in a secure manner. This includes review and test of all Data Importer applications, products and services for common security vulnerabilities and defects, employing defense-in-depth strategy through the use of multiple layers of security boundaries and technologies, periodic pen testing and security assessment of these services, defining baseline configurations and requirements for patching of third party systems.

4.3 Data Protection

4.3.1 Data Isolation

The Data Importer logically isolates the Data Exporter's data, and the Data Exporter has a large degree of control over the specific data stored in the Service.

4.3.2 Data in Transit

Interactions between users, administrators and Corrily's dashboard are done using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) standard cryptographic protocols.

Corrily's API is accesses through publically available endpoints but encrypted through the user of client-specific API keys.

4.3.3. Data at Rest

The Data Importer uses cryptographic hashing and encryption mechanisms to protect sensitive

4.3.5 Data Deletion.

The Data Importer provides to the Data Exporter a mechanism that can be used to delete the Data Exporter's data.

4.3.6 Personal Data Incident Management and Notification

Data Importer will implement and maintain a data security incident management program that addresses management of data security incidents including a loss, theft, misuse, unauthorized access, disclosure, or acquisition, destruction or other compromise of Personal Data. Except to the extent necessary to comply with applicable legal, regulatory or law enforcement requirements, Data Importer will inform you without unreasonable delay in accordance with Applicable Law after it becomes aware of any Incident that has occurred in its systems which affects Personal Data Data Importer processes on your behalf.

4.2 Human Resources Security

Data Importer shall maintain a policy which defines requirements around enforcing security measures as they relate to employment status changes. This includes background checks, acknowledgement and adherence to Data Importer's security policies, onboarding and termination for employees and third parties.

4.3 Network Security

Interactions between users, administrators and Data Importer modules are done using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) standard cryptographic protocols. The Data

Importer employs multiple layers of DOS protection, Intrusion Detection, Rate Limiting and other network security services from both its hosting providers and third party providers. The Data Importer makes HTTPS encryption available.

4.4 Sub-processor Security.

Prior to onboarding sub-processors that will handle any data provided by a Data Exporter, the Data Importer conducts an assessment of the security and privacy practices of the sub-processor to help ensure that the sub-processor provides a level of security and data protection controls appropriate to their access to data and the scope of the services they are engaged to provide.

4.5 Business Continuity and Disaster Recovery

Data Importer shall maintain policies and procedures to ensure that Data Importer may continue to perform business critical functions in the face of an extraordinary event. This includes data center resiliency and disaster recovery procedures for business-critical data and processing functions.

Schedule 4
AUTHORISED SUBCONTRACTORS

Subcontractors	**Services provided**	**Contact Details**
Google Cloud Platform	Cloud Computing / Data Warehouse and Analytics Services	1600 Amphitheatre Parkway Mountain View, CA 94043
Hasura	Data Warehouse Services	355 Bryant Street, Suite 403, San Francisco CA 94107
Auth0	Dashboard User Management	10800 NE 8th Street Suite 700 Bellevue, WA 98004