Data Privacy and Security Addendum

Exhibit D of the Master Services Agreement signed on XXX XX, 2023
By:

YALO ENTITY Hereinafter Yalo	xxxxxxxxxxxxxx Hereinafter the Client

Yalo and Client hereinafter each a Party or Data Controller and together the Parties or the Data Controllers

This Data Security & Privacy Addendum (this "Addendum"), effective as of [DATE] ("Addendum Effective Date"), forms a part of the Yalo Master Service Agreement ("MSA") or Yalo Statement of Work ("SOW") entered into by and between the Data Controllers and q, dated as of [DATE], and may be amended or supplemented from time to time (the "Agreement") over the course of providing the Services defined in the Terms and Conditions of (the "Agreement"). The Parties have agreed to enter into this Agreement in order to address the compliance obligations imposed to the Parties pursuant to the Applicable Privacy Law, including, but not limited to, the Brazilian General Data Protection Law (Law 13,709/2018 or LGPD), as per defined below, and to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data.

In consideration of the matters described above, the Data Controllers agree as follows:

1. DEFINITIONS

1.1. "Applicable Privacy Law" means all laws, statues, regulations, ordinances, codes, rules, guidance, orders or any other legal entitlement issued by any governmental body governing the collection, use, transfer, and disclosure of Personal Data in which the Data Controllers operate or collect Personal Data from as set out in Schedule D, solely in respect to the Processing Activities set out in the MSA or SOW, and solely in respect to the jurisdictions from which the Personal Data is collected.

1.2. "Applicable Law" means all laws, statues, regulations, ordinances, codes, rules, guidance, orders or any other legal entitlement issued by any governmental body governing the Data Controllers that is of general application to entities operating within the jurisdictions that Data Controllers operate or as identified in the Master Service Agreement (MSA) or Statement of Work (SOW) made pursuant to it.

1.3. "Affiliated Companies" means any legal entities controlling, controlled by or under common control with a Data Controller as set out in the Master Service Agreement (MSA).

1.4. "Data Controller" means the party that has authority over the processing of personal information, determining the purpose for its use and the manner that it is processed.

1.5. "Data Processor" means the party that processes Personal Data on behalf of, and under the instruction of, the Data Controller.

1.6. "Data Protection Authority" means the official body that ensures compliance of the Applicable Privacy Law within its applicable jurisdiction.

1.7. "Data Subject" means the directly or indirectly identified or identifiable person to whom the Personal Data relates.

1.8. "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed, excluding Personal Data which is encrypted or tokenized, for which the password, token, security key or device to decrypt such Personal Data has not been the subject of any loss or disclosure.

1.9. "Brazilian General Data Protection Law" and "LGPD" means Law No. 13,709/2018 its subsequent amendments, and any other laws and regulations regarding the processing, protection and privacy of Personal Data that may be applicable and, if applicable, all guidelines, rules, ordinances, regulations and codes of practice and conduct issued by the Data Protection Authority or other relevant Personal Data protection or supervisory authority.

1.10. "Personal Data" means any information regulated by Applicable Privacy Law provided by the Data Controllers, including information concerning an identified or identifiable individual, such as, name, address, age, gender, income, family status, health records, etc

1.11. "Processing" means any operation performed with personal data, such as those that concern the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or information control, modification, communication, transfer, dissemination, or extraction.

1.12. "Schedule" means the schedules to the DPA.

1.13. "Sub-processor" means third-party Data Processor engaged by Data Processor who has or potentially will store, have access to, or processes Personal Data.

1.14. “Sensitive Personal Data” means personal data on racial or ethnic origin, religious belief, political position, membership in a trade union or affiliation to religious, philosophical, or political organization, data concerning health or sexual life, genetic or biometric data, when linked with an individual.

1.15. “Services” means the services provided to the Client by Yalo pursuant to the MSA and the Yalo Statement of Work (“SOW”)

1.16. "Technical and Organizational Security Measures" means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.

1.17. “Transfer” means to disclose or otherwise make Personal Data available to a third party (including to any Affiliate or Subprocessor), either by physical movement of the Personal Data to such third party or by enabling access to the Personal Data by other means.

All other terms expressed in capital letters not explicitly defined under this Agreement, shall have the meanings given to them by the Applicable Privacy Law.

2. PURPOSE(S) OF THE PROCESSING OF PERSONAL DATA

2.1. Both Yalo and the Client act as Controllers and must process any Personal Data in their possession in accordance with the LGPD. The purpose(s) of the processing of both the DPA and the MSA are specified in Schedule A, and shall be restricted to the limits set forth by the Applicable Privacy Law. Each party represents and warrants it has full authority to issue binding instructions and/or guidance to the other party, regarding the nature, scope and procedure of the data processing activities. Instructions must be granted in a documented form (i.e. in writing, including via email).

.

2.2. Each Party agrees that the other Party may use the names, phone numbers, business addresses, and e-mail addresses of its employees (Business Contact Information) for contract management, payment processing, service offerings and such other purposes as set out in the using Party’s privacy notice (copies of which shall be made available upon request), subject to compliance with the applicable laws. For such purposes, and notwithstanding anything else set forth in this DPA, or any Statement of Work (SOW) pursuant to the MSA, with respect to Personal Data in general, each Party shall be considered a Data Controller with respect to the other Party’s Business Contact Information and shall be entitled to transfer such information to any country where such Party’s organization operates. Each Party warrants that it has authority to consent to the use of the Business Contact Information by the other Party.

2.3. The Client recognizes the principal purpose for the Services under the MSA and the Yalo Statement of Work (SOW) is to support communications between the Client and its customers through the Data Processor’s Messaging Platform (as defined in the MSA and Yalo Statement of Work (SOW). Client acknowledges further that due to the nature of the Services provided, that Yalo and its sub-processors may not be aware of whether Personal Data has in fact been stored in its systems, and do not regularly access any Personal Data that may be resident on Yalo’s systems. Furthermore, Yalo itself has procedures to ensure that though programmatically the Yalo’s Services can access Personal Data stored within the Services, that such access is limited to key individuals and is not available to Yalo’s staff, employees and contractors generally except solely on the basis of need to know for the performance of administrative and operational responsibilities as a data custodian, to facilitate professional services, customer support or security incident response.

2.4. If any of the Parties is required to disclose Personal Data to the Data Protection Authority or pursuant to an order of a court or tribunal of competent jurisdiction, it shall inform the other Party of that legal requirement before disclosing the Personal Data concerning the Services Provided, unless applicable law prohibits such information on important grounds of public interest, or to support its legitimate interests in complying with laws of general application on the part of the involved Party.

2.5. The Client and Yalo agree to process information, including Personal Data, necessary to maintain and improve the Services , and to utilize anonymized and aggregated data, as set out in section 5.3 of the MSA for Yalo’s own purposes. The processing activities related to maintenance, quality control and improvements of the Services shall in any event be conducted by the responsible Party of the database subject to its obligations under this Exhibit and the Applicable Privacy Law.

3. CLIENT’S OBLIGATIONS

The Client shall, working in cooperation with Yalo:

3.1. Apply data minimization principles in the collection, use or storage of such Personal Data in Client’s use of the Services provided under the Statement of Work (SOW), that are actually required to utilize the required Services, acknowledging that the data collection done through the Services may be undertaken with a minimal set of personal data elements;

3.2. Utilize secure methods for the transmission and sharing of Personal Data with Data Processor (if any), appropriate to its sensitivity;

3.3. Maintain and keep secure passwords and tokens utilized to access the Services;

3.4. Manage, using the portal and tools provided by Yalo, its own retention of data, including secure disposal or deletion of such Personal Data;

3.5. Make reasonable efforts to ensure that the Client can comply with the contractual obligations resulting from this Agreement.

3.6. Respond to inquiries from Data Subjects, the Data Protection Authority and/or competent authorities in relation to the Processing of Personal Data. Responses will be given within a reasonable time, in accordance with the Applicable Privacy Law.

3.7. Maintain records of Processing of Personal Data, as well as any other records, documents, or inventories, in accordance with any Applicable Privacy Law and disclose them to Yalo upon reasonable request.

3.8. Establish authentication mechanisms for access to records, using, for example, two factor authentication systems to secure the individualization of the person responsible for Processing data.

3.9. Take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know/access the relevant Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with all laws, including Applicable Privacy Law, in the context of that individual's duties of each other, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

3.10. Create a detailed inventory of accesses to connection and access to applications records, containing the time, duration, identity of the employee or the person responsible for access designated by the Client and the file accessed, even when such access is made to comply with the legal obligations or determinations by authorities;

3.11. Implement appropriate Technical and Organizational Security Measures to ensure appropriate security of the Personal Data (including protection from unauthorized, accidental or unlawful destruction, loss, alteration, disclosure of, or access to Personal Data transmitted, stored or otherwise Processed) including, as applicable: (i) the pseudonymization and encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

3.12. Immediately notify Yalo within a maximum period of 24 hours about (a) any summons, demands, requests for judicial cooperation regarding the disclosure of Personal Data; (b) any accidental or unauthorized access to Personal Data; (c) any requests by Data Subjects that may potentially involve Yalo, before answering it, unless expressly authorized to do so.

3.13. Maintain Yalo informed of all existing subcontractors that will process Personal Data connected with this Agreement and provide updates if new hires occur.

3.14. Not use any type of tool, technology, reverse engineering or any other method aimed at identifying the Subjects of Personal Data in cases where Yalo has shared Anonymized Personal Data.
The Client represents and warrants that the Personal Data is being processed lawfully in accordance with the Applicable Privacy Law or laws and regulations applicable in which the Personal Data is derived, or to which the Client is subject.

4. YALO'S OBLIGATIONS

Yalo shall:

4.1. Take all security measures required pursuant to Applicable Privacy Law . Technical and operational security measures are set out in Schedule B.

4.2. Provide, with no additional cost, all the necessary information to demonstrate compliance under the Applicable Privacy Law.

4.3. Notify the Client of any relevant change in laws applicable to the data Processing that would prevent either of the Parties from performing their obligations under this DPA in compliance with the Applicable Privacy Law or that would require modifications or further actions.

4.4. Ensure that Personal Data is only being collected, used and processed as required in Schedule A. In case Yalo becomes aware that it has received additional information that is not needed to provide the Services, it must inform the Client within five (5) business days, and stop the processing of the additional Personal Data.

4.5. Guarantee that all personnel with access to the Personal Data are legally bound by confidentiality obligations during and after the termination of the DPA, including after the termination of their employment.

4.6. Train its employees involved in the processing of the Personal Data to comply with the Applicable Privacy Law and with the requirements established in this DPA

4.7. Provide access to its employees on a need-to-know basis only, and make sure that the employees are aware and compliant with the MSA, the DPA and the Applicable Privacy Law.

4.8.
Assist the Client, insofar as this is possible, to respond to any Data Subject's request exercising their rights in accordance with LGPD or other Applicable Privacy Law.

4.9. Designate a Data Processor Contact (DPO), where required by Applicable Privacy Law.

5. DATA PROCESSORS AND SUB-PROCESSORS

5.1. Any of the Parties shall require written approval from the other Party to contract with Data Processor or Sub-processors to handle the Personal Data.

5.2. A list of approved Data Processor or Sub-processors is included in Schedule C; the Party consents to the use of the Data Processor or Sub-processors set out in Schedule C.

5.3. The obligations and specifications included in the DPA will apply to the Data Processors and Sub-processor when handling the Personal Data.

5.4. The involved Party will annually assess and validate each Data Processor’s or Subprocessor’s capacity to comply with the obligations of the DPA.

5.5. The other Party shall be notified of any deficiencies or non-compliance of existing Data Processor or Sub-processors and decisions to engage any new Data Processor or sSubprocessor upon which the Services is dependent.

6. RIGHTS OF DATA SUBJECTS

The Parties should assist each other in fulfilling its obligations to facilitate the exercise of Data Subject rights under the Applicable Privacy Law.

7. RESPONDING TO DATA SUBJECT REQUESTS

The Parties shall transfer to each other any request received from the Data Subjects within (10) business days, unless a shorter period is prescribed by the Applicable Law, and will inform the Data Subjects that they can direct their requests directly to the responsible Data Controller. Yalo will only handle the requests according to the Client’s instructions; however, Yalo shall only be obliged to respond to requests relating to the processing that Yalo is responsible for under its agreement with the Client.

8. NOTIFIABLE DATA BREACHES

8.1. The Parties shall notify each other without undue delay within (24) hours of confirmation of a Data Breach. The notification shall include:

8.1.1. Description of the Data Breach, including, if possible, the categories of data and records concerned, the category and number of Data Subjects affected.

8.1.2. Likely consequences of the Data Breach.

8.1.3. Measures taken or proposed to address and/or mitigate the effects of the Data Breach.

8.1.4. Name and contact of the Data Protection Officer or Privacy Officer, or any contact point where further information can be reached.

8.2. The Data Privacy and Security Contacts from both Parties shall cooperate to comply with the obligation to notify the Data Protection Authorities and Data Subjects under the Applicable Privacy Laws.

8.3. The affected Party shall, with undue delay, take all urgent measures to invoke breach response protocol to contain the Data Breach and protect the Personal Data.
8.4. Parties need the previous approval of the other Party to include and identify them in the breach notifications. Parties should not delay or withhold the approval without a reasonable cause.

9. COOPERATION

9.1. Upon request, the Parties shall assist each other to comply with its obligations under the LGPD when related to the processing of the Personal Data, including but not limited to:

9.1.1. Data Breaches.

9.1.2. Data Protection Impact Assessments.

9.1.3. Enquiries, complaints, audits, or claims from any court, government official, Data Protection Authority, third parties or individuals (including but not limited to the Data Subjects).

9.2. The Parties shall make available to each other all information necessary to comply with its obligations under the DPA and the Applicable Privacy Law.

9.3. The Parties shall notify the other Party of any requirements from an official authority within forty-eight (48) hours of receiving said enquiry, subject to section 2.4.

10. AUDIT RIGHTS

10.1. The Parties shall comply with the obligations and requirements provided by Applicable Privacy Law in order to Process, Transfer or in any manner handle Personal Data
10.2. Upon advanced written previous notice, and no more than once a year, the Client may request that it conduct an audit at its own expense to verify the Yalo’s compliance with the DPA. Approval of such audit shall be solely within the discretion of Yalo.

10.2.1. The Client may do one (1) yearly audit in case of a Data Breach or a security incident affecting the Client’s data.

10.2.2. The Client shall schedule the audit with Yalo at least 4 weeks in advance.

10.2.3. Both Parties shall agree upon the scope, the timing, and the duration of the audit.

10.2.4. The Client shall notify Yalo of information regarding any non-compliance discovered during an audit, and any reports or remediation shall be considered Yalo's confidential information.

10.2.5. Yalo, depending on the scope, duration and staffing resource impact on Yalo, may charge a fee in relation to the Client's audit.

10.3. The audit might be carried out by the Client directly or by a third-party auditor appointed by the Client.

11. DATA PRIVACY AND SECURITY CONTACTS

For Yalo:

Name	
Address	
Email	
Telephone	

For the Client:

Name	
Address	
Email	
Telephone	

12. TERMINATION FOR CAUSE

12.1. Each Party Has the right to terminate the DPA for cause if the other Party Infringes in a substantial manner the following provisions:

Sections 5 — Data Processor Obligations;
Section 3 — Instructions;
Section 6 — Subprocessor
Section 9 — Notifiable Data Breaches;
Section 10 — Cooperation;
Section 11 — Audit Rights.

12.2. Statutory rights to terminate for cause shall remain unaffected.

13. RETURN AND DELETION OF PERSONAL INFORMATION

13.1. Yalo shall return or irrevocably delete or remove the Personal Data upon termination of the DPA, unless storage of the Personal Data is required by the Applicable Privacy Law.

13.2. Yalo shall provide certification of the deletion, removal or return of the Personal Data. The Client has the ability to delete and remove documents containing Personal Data through the tools provided by Yalo.

14. LIABILITY

14.1. 14.1 Yalo's liability to the Client, its affiliates, their officers, agents, employees under this Agreement shall be limited to the amount of one (1) year's subscription to Yalo's Master Service Agreement (MSA).

15. CYBER SECURITY INSURANCE

15.1. The Parties shall purchase adequate cyber security insurance to cover all liability that might arise under the DPA and ensure that the cyber security insurance is in full force and effect throughout the life of the DPA.

.

15.2. The Parties shall make sure that their respective Data Processor or Sub-processors are insured to appropriate levels if relevant to their services.

16. JURISDICTION

16.1. This DPA will be governed by the governing law of Brazil.

17. NOTICES

18.1 Any notice between the Parties shall be in writing to the following addresses:
18.1.1 Yalo:

Address	
Email	

18.2 The Client:

Address	
Email	

18. ENFORCEABILITY

18.1. Should any provision of this DPA be or become, either in whole or in part, void, ineffective or unenforceable, then the validity, effectiveness and enforceability of the other provisions of this DPA shall remain unaffected thereby.

18.2. Any such invalid, ineffective or unenforceable provision shall, to the extent permitted by law, be deemed replaced by such valid, effective and enforceable provision as most closely reflects the economic intent and purpose of the invalid, ineffective or unenforceable provision regarding its subject-matter, scale, time, place and scope of application.

18.3. The aforesaid rule shall apply *mutatis mutandis* to fill any gap that may be found to exist in this DPA.

19. ENTIRE AGREEMENT

Parties explicitly declare that this DPA and the documents referred to herein constitute the entire agreement between Parties and supersedes any prior draft, agreements, undertakings, understandings, conditions and arrangements, notwithstanding any conflicting order of precedence, of any nature between the Parties, whether or not in writing, in relation to the subject-matter of this DPA.

IN WITNESS WHEREOF, [___] and [___] have caused this DPA to be signed by their duly authorized representatives.

[___]:	[___]:
Signature	Signature
Print Name	Print Name
Title	Title
Date	Date

Index of Schedules:

Schedule A: Purpose of Data Processing, Data Categories and Data Subjects
Schedule B: Technical and Operational Security Measures
Schedule C: Approved Sub-processors and supporting services
Schedule D: Applicable Law - Jurisdictions

Schedule A – Purpose of Data Processing, Data Categories and Data Subjects

The extent, type and purpose of the Processing is as follows:

- Yalo will collect limited Personal Data as needed to support the Client's use of its Services.

This excludes data processed by Data Processor pursuant to section 2.3.

Description	Details
Subject matter of the processing	Yalo is a provider of a Messaging Platform (as defined in the MSA). Client has purchased a subscription for the Yalo's services pursuant to the terms set out in the Services Agreement for services between the the Parties, in accordance with which Personal Data may be hosted by the Yalo Including via its sub processors.
Type of Personal Data	Any Data Subjects who may use the chat functionality to communicate with the Yalo or the Client, which may include: employees, agents and subcontractors; customers and their employees, agents, and subcontractors including those of other third parties whom the Clients have a business interest in or business relationship with (collectively referred to as "Users").
Categories of Data Subject	Personal data may be contained in the messages sent by Users through the Messaging Platform, which relate to the Client's clients and/or their customers, employees and other persons the clients have a business interest in or business relationship with.
Nature and purposes of the processing	Personal data will be processed on the Yalo's chat Messaging Platform once uploaded by a User. In addition, as part of providing technical help desk support, the Yalomay access personal data through remote screen share, email and telephone with Users.
Duration of the processing	The term of this Agreement, or subject to deletion by as provided in the MSA
Location of Processing	Region specified on Statement of Work (SOW)
Return and destruction of data	Personal data delivered or generated will be returned to the Client within a period not exceeding 90 days after the termination of the contract, including proof of deletion. An extension of the time may be made with a mutual written agreement of the parties.

Schedule B – Technical, Administrative and Operational Security Measures

Security Program

Yalo will maintain a written information security program of policies, procedures and controls that directly align with certification and attestation objectives stated in SOC 2 Type 2 trust service principles for “Security” or equivalent standards.

Accreditation & Certification

Yalo maintains compliance with industry recognized frameworks SOC 1 and SOC 2 type 2, under which Yalo implements and maintains reasonable physical, administrative, and technical safeguards designed to protect the security of Yalo Messaging Platform following trust services criteria for ‘Security’.

Yalo regularly evaluates these safeguards, and may review and update its security program, policies or procedures as well as this Addendum, provided that such updates shall be designed to enhance and not materially diminish the security program.

Yalo Messaging Platform shall be regularly assessed by independent third-party auditors on at least an annual basis for the following audits and certifications:

- SOC 2 Type I
- SOC 2 Type II

Control	Control Mechanism	Details
Design control	Data minimization	• Users are able to provide information based on needs for communication with the Data Controller. • Usage data and analytics are minimal, and are aggregated (e.g. trends), data is collected.
Disclosure Control	Encryption at Rest/ Encryption in Transit	• Data stored within Data Processor’s application is encrypted • All transmissions through application with Controller or through reporting dashboards are encrypted. • Access to data is restricted
Monitoring	Logging	• Logging/audit reporting systems exist to validate direct and indirect access to data, which includes OS-level access logging, real-time monitoring • Access to data is restricted and logged
Limit on sharing	Controller Access Controls	• Specified contacts within Data Controller are the only ones able to access or create data within Data Processor’s systems.
Limit on access	Processor Access Controls: Acceptable Use Policy	• Support staff ability to access data is limited to need to know for the performance of administrative and operational responsibilities as a data

		custodian, to facilitate professional services, customer support or security incident response. ● Full logging of all access. ● Acceptable Use Policy ● Data Classification and Handling Standards
Limit on retention	Retention Policy	● Retention is limited to the period of time required by the Data Processor to comply with legal obligations or business purpose of agreement, and only for data that is required to be collected. ● Data Controller has the ability to delete data through the Services provided by the Data Processor at any time.
Accountability	Code of Conduct	● Code of Conduct requires employees to comply with Data Processor security and privacy policies and procedures
Accountability	Data Flow	● Data flow is documented and updated as changes are made to application
Accountability	Sub-processor Contracts Standard Contractual Clauses	● Contracts in place with sub-processors providing limits on use and access to data. ● Standard contractual clauses or equivalents used where appropriate.
Limit on sharing	Segregation Control	● Controller Data is logically separated. When personal data is stored it is either, Stored in a structured logical database by “Data Controller” or stored in an independent, operational database in the instances of Data Processors products providing services.
Availability	Business Continuity	● Backup procedures ● Uninterruptible power supply (UPS) ● Remote storage ● Antivirus/firewall systems ● Disaster recovery plan
Access Control to	Physical Security	● Access Control to AWS and Google Data Center site is controlled by AWS and

Premises & Facilities		Google as a subservice provider. • AWS provides numerous certifications and assessments to support effectiveness of physical and environmental controls.
Access Control to Systems	Technical and organizational user controls	• Access control to hosting facilities is managed by Data Processor's sub-processor, AWS and GCP, to which both sub-processors must maintain compliance with SOC procedures for control and audit. • No Personal data is stored at office facilities or on systems hosted on premises. • Password procedures (incl. special characters, minimum length, change of password) • Automatic blocking (e.g. password or timeout) • Encryption of data media
Access control to data	Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses:	• Differentiated access rights (profiles, roles, transactions and objects) ○ Reports Access ○ Change ○ Deletion • Data changes and associated access requests are logged.

Schedule C: Approved Sub-processors and Supporting Services

The following table describes the countries and legal entities engaged in storage, processing and handling of data by the Parties. This includes organizations that are providing services or tooling that are essential in the delivery of Processors platform and services.

#	Entity Name	Entity Type	Area of Use
1	Amazon Web Services Inc.	Sub-Processor Cloud Service Provider	Amazon Web Services (AWS) is used for product hosting and data storage for Yalo's customer integrations, including security services.
2	Google Cloud Platform (GCP)	Sub-Processor Cloud Service Provider	Google Cloud Platform is used for product hosting and data storage for Yalo's platform infrastructure.
3	Cloudflare	Supporting Service	DNS provider
4	Kong Inc.	Supporting Service	API Gateway Provider
5	Auth0	Supporting Service	Authentication and authorization service that integrates with external data controllers identity providers.
6	Bitbucket	Supporting Service	Central management of Yalo source code. Provides version and change control functionality for software development and release process.
7	Github	Supporting Service	Central management of Yalo source code. Provides version and change control functionality for software development and release process.
8	Datadog	Supporting	Observability service for

		Service	cloud-scale applications, providing monitoring of tools and services, through a SaaS-based data analytics platform.
9	Confluent	Supporting Service	Message broker service
10	Meta	Supporting Service	- Facebook messaging platform - WhatsApp Business Platform - WhatsApp API
11	Rocketchat	Supporting Service	Opensource communications platform.
12	Twilio	Supporting Service	Segment - customer data platform
13	Split	Supporting Service	Feature delivery platform
14	Salesforce	Supporting Service	- Salesforce SFDC/CRM - Slack Communications Platform
15	FrontApp	Supporting Service	Collaborative messaging platform.
16	Atlassian	Supporting Service	- Jira issue tracking - Bitbucket - source code management & version control

Schedule D: Jurisdictions of Origin

(to be completed as required)