DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is made by and between the Customer ("**Controller**" or "**Customer**") and Blinks Labs GmbH, located at Sonnenallee 223, 12059 Berlin, Germany ("**Processor**" or "**Blinkist**") (each a "**Party**", and together the "**Parties**").

RECITALS

WHEREAS, the Customer has entered into a customer contract for the Services with Blinkist or an Affiliate of Blinkist ("**Agreement**").

WHEREAS, in the course of providing the Services to Controller pursuant to the Agreement, Processor may Process Personal Data on behalf of Controller;

WHEREAS, to ensure adequate safeguards with respect to the Processing of Personal Data provided by Controller to the Processor the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

NOW, THEREFORE, in consideration of the foregoing premises and of the mutual promises and covenants set forth below, Controller and Processor hereby agree as follows:

AGREEMENT

1. DEFINITIONS

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. The term "**Control**", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Applicable Data Protection Laws**" means all applicable laws, regulations, regulatory guidance, or requirements in any jurisdiction relating to data protection, privacy, or confidentiality of Personal Data of the European Union, the European Economic Area and their Member States, Switzerland, the United Kingdom, Canada, Israel, Australia and the United States of America, as applicable to the Processing of Personal Data under the Agreement including but not limited to the EU GDPR, the UK GDPR, the Swiss FADP as well as the Californian CCPA and CPRA.

"Blinkist Services" means all services provided by Blinkist online, via app or other means.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations.

"**Client Data**" means any Personal Data that the Processor handles and for which the Customer is the Data Controller.

“Controller” means the entity which determines the purposes and means of the Processing of Personal Data. For the avoidance of doubt, the Party identified as Controller above is a Controller under this DPA.

“Data Breach” means a breach of security leading to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed.

“Data Protection Authority” means any representative or agent of a government entity or agency who has the authority to enforce Applicable Data Protection Laws.

“Data Subject” means a natural person to whom Personal Data relates.

“End User” means a user of the Blinkist Services or library of content therein.

“EU GDPR” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), together with any transposing, implementing or supplemental legislation.

“**FADP**” means the Federal Act on Data Protection of 19 June 1992, and as revised as of 25 September 2020.

“Personal Data” means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

“Process” shall mean any operation or set of operations which is performed upon Personal Data, whether or not accomplished by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; and as defined by Applicable Data Protection Laws.

“Processor” means the entity which Processes Personal Data on behalf of the Controller. For the avoidance of doubt, the Party identified as “Processor” above is a Processor for this DPA.

“Services” means Processing of Personal Data by the Processor in connection with and for the purposes of the provision of the services to be provided by the Processor pursuant to the Parties Agreement.

“Service Provider” means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that process information on behalf of a Data Controller and to which the Data Controller discloses a Data Subject’s Personal Data for a Business Purpose pursuant to a written contract, provided that the contract prohibits the Service Provider from retaining, using, or disclosing the Personal Data for any purpose other than for the specific purpose of performing the services specified in the contract, or as otherwise permitted by the CCPA, including retaining, using, or disclosing the Personal Data for a Commercial Purpose other than providing the services specified in the contract with the Data Controller. The terms “Business Purpose” and “Commercial Purpose” have the same meaning as those terms are used in the CCPA. For the avoidance of doubt, Processor is a Service Provider.

"Sub-processor" means any entity which Processes Personal Data on behalf of the Processor.

"**UK GDPR**" means the Data Protection Act 2018, as well as the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

2. PROCESSING OF PERSONAL DATA

2.1. **Details of the Processing.** The subject matter, duration, purpose of the Processing, and the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1.

2.2. **Controller's Obligations.** Controller's instructions for the Processing of Client Data shall comply with Data Protection Laws and Regulations. Controller shall have sole responsibility for the accuracy, quality, and legality of Client Data and the means by which Controller acquires Client Data and provides it to Processor. Controller shall also be solely responsible for safeguarding the rights of Data Subjects.

2.3. **Processor's Instructions.** All Client Data Processed by Processor pursuant to the Agreement is Confidential Information and Processor will Process Client Data only in accordance with Controller's documented instructions set forth in this DPA or as otherwise provided by Controller in writing. Insofar as the Processor is required to process the Client Data without any instruction from the Controller by Union or Member State law to which the Processor is subject, the Processor shall inform the Controller of that legal requirement in due time before processing, unless that law prohibits such information on important grounds of public interest. Processor shall adhere to all Applicable Data Protection Laws regarding to Processing Personal Data. Where the Processor believes that compliance with any instructions by Controller would result in a violation of any Applicable Data Protection Law, the Processor shall notify Controller thereof in writing without delay.

2.4. **Assistance Requirements.** Processor shall assist Controller in ensuring compliance with the obligations set out in Applicable Data Protection Laws, especially with the following: security of Processing, handling of (suspected or known) Data Breaches; notifications to, or inquiries from a Data Protection Authority; notifications to, and inquiries from, Data Subjects; and performance of data protection impact assessments and prior consultations with a Data Protection Authority.

2.5. **End-User Relationship.** Where Processor Processes Personal Data in the context of a direct relationship with an End User in the course of providing or offering services to them, such Processing is outside the scope of this DPA.

2.6. **Processor's Obligations regarding the CCPA.** Insofar as the Client Data includes Personal Data protected under the CCPA, the Processor will not:

2.6.1. retain, use, disclose or otherwise Process such Client Data other than for the limited and specified purposes identified in this DPA, the Agreement, and/or any related project order;

2.6.2. retain, use, disclose or otherwise Process such Client Data for a commercial purpose other than for the limited and specified purposes identified in this DPA, the Agreement, and/or any related project order, or as otherwise permitted under the CCPA;

2.6.3. "sell" or “share” such Client Data within the meaning of the CCPA;

2.6.4. retain, use, disclose or otherwise Process such Client Data outside the direct business relationship with the Controller and not combine such Client Data with personal data that it receives from other sources, except as permitted under the CCPA; and

2.6.5. attempt to re-identify any pseudonymized, anonymized, aggregate, or de-identified Client Data without the Controller’s express written permission.

3. NOTIFICATION OBLIGATIONS

3.1. **Processor’s Notification Obligations.** Processor shall immediately notify Controller, in writing, of the following:

3.1.1. A Data Subject’s request to exercise their privacy rights such as accessing, rectifying, erasing, transporting, objecting to, or restricting their Personal Data;

3.1.2. Any question, complaint, investigation, or other inquiry from a Data Protection Authority;

3.1.3. Any request for disclosure of Personal Data that is related in any way to Processor’s Processing of Personal Data under this DPA;

3.1.4. A Data Breach pursuant to the notification obligations set forth in Section 7.1; and

3.1.5. Processor will assist Controller in fulfilling Controller’s obligations to respond to requests relating to sections (3.1.1)-(3.1.4) above and will not respond to such requests without prior consultation with the Controller, unless Processor is required to respond by applicable law. If a Data Subject addresses the Processor directly in the exercise of their privacy rights, the Processor shall immediately forward this request to the Controller and support the Controller in a reasonable manner with appropriate technical and organizational measures to comply with his obligation to respond to such requests for the exercise of the rights of the Data Subject.

4. CONFIDENTIALITY

Processor’s Personnel. Processor shall ensure that its personnel engaged in the Processing of Client Data are informed of the confidential nature of the Client Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Processor shall ensure that such confidentiality obligations survive the termination of their respective employment relationship with such individuals.

5. SUB-PROCESSORS

5.1. **Appointment of Sub-processors.** Controller acknowledges and agrees that Processor and Processor’s Affiliates may engage third-party Sub-processors in connection with the provision

of the Services. For the time being, Processor engages the Sub-processors listed in Schedule 3. Processor or Processor's Affiliate shall enter similar data protection obligations with each Sub-processor as set out in this DPA.

5.2. **Notification of Changes to Sub-processors.** Processor will inform Controller of any intended changes concerning the addition or replacement of Sub-processors and give Controller an opportunity to object to such changes. Processor will notify Controller of any intended changes concerning the addition or replacement of Sub-processors at least thirty (30) days prior to its use of the Sub-processor.

5.3. **Objection Right for New Sub-processors.** Controller may object to Processor's use of a new Sub-processor by notifying Processor promptly within fifteen (15) business days after receipt of Processor's notice. Unless Controller objects within the aforementioned period, the change shall be deemed to have been approved by Controller. Processor shall inform Controller of this significance of its conduct at the beginning of the period. In the event Controller objects to a new Sub-processor, Processor may, at its own discretion, either provide the service without the intended change, or – if the provision of the service without the intended change is not reasonable for the Processor – discontinue the service to the Controller within two weeks of receipt of the objection and terminate the Agreement without notice and with immediate effect.

5.4. **Third country transfers.** Should the engagement of a Sub-processor lead to a transfer of Client Data to a country outside of the European Union (EU) or the European Economic Area (EEA) ("**Third Country**"), clause 9.1. of this DPA applies.

5.5. **Liability for Acts of Sub-Processors.** Processor shall be liable for the acts and omissions of its Sub-processors to the same extent Processor would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY AND AUDIT

6.1. **Protection of Personal Data.** Processor shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the Processing. These measures shall include the ability to restore the confidentiality, the integrity, the availability and the resilience of the systems permanently and to restore the availability of and access to personal data quickly after a physical or technical incident. Processor shall regularly review, assess and evaluate the effectiveness of the technical and organizational measures taken to grant the security of the processing and document the results. The Parties agree that the technical and organizational measures listed in Schedule 2 to this Agreement are appropriate to the risk of the data processed on behalf of the Controller. The Processor undertakes to implement the measures listed in Schedule 2 to this Agreement prior to the start of the Processing of Client Data, maintain them for the duration of the Processing and, if necessary, adapt them to the state of the art and the risk of the Processing.

6.2. **Audit Rights.** Processor shall grant the Controller the right to evaluate the Processing and the compliance with this Contract. In particular, Processor shall provide Controller with all information required to prove compliance with the obligations laid down in this Agreement and shall enable the execution of evaluations, including inspections. These audits may also be carried out by a third party obliged to confidentiality, provided that the third party is not a

competitor of Processor. The parties agree that Controller shall conduct an evaluation by instructing Processor, at the Processor's option, to submit an appropriate audit report or extracts of reports from independent bodies (e.g. auditors, data protection officers, data protection auditors or quality auditors) or an appropriate certification by an IT security or data protection audit ("**Audit Report**"). Notwithstanding, Controller may conduct an independent inspection when reasonably justified. Processor shall support Controller in its evaluation. This includes granting the Controller all access, information and inspections rights. The same applies to evaluations conducted by Data Protection Authority in accordance with the applicable data protection regulations. Controller shall inform Processor about all circumstances relating to the conduct of the evaluation in due time (generally at least four weeks prior to the evaluation). Generally, Controller may conduct an evaluation once per calendar year. Notwithstanding the foregoing, Controller shall have the right to conduct further evaluations in the event of special occurrences.

7. DATA BREACHES

7.1. **Data Breach Notification.** Processor shall notify Controller in writing without undue delay after becoming aware of a suspected Data Breach. Within this notification, the Processor shall inform the Controller as comprehensively as possible about the nature and extent of the incident and the time it occurred, the IT system and data subjects affected, the time of discovery, all conceivable adverse consequences of the Data Breach and the measures taken as a result.

7.2. **Data Breach Management.** Processor shall make reasonable efforts to identify the cause of such Data Breach and take those steps as Processor deems necessary and reasonable to remediate the cause of such a Data Breach to the extent the remediation is within Processor's reasonable control.

8. TERMINATION

8.1. **Termination.** This DPA shall terminate automatically upon the later of (a) the termination or expiry of the Agreement or (b) Processor's deletion or return of Personal Data.

8.2. **Return or Deletion of Data.** Upon termination of this DPA, Processor shall, at the choice of Controller, delete or return all Client Data to Controller, unless applicable law requires continued retention of the Personal Data. In instances where applicable law requires the Processor to retain Client Data, Processor will protect the confidentiality, integrity, and accessibility of the Client Data.

9. MECHANISMS FOR INTERNATIONAL TRANSFERS

9.1. **Transfers Outside of the EU.** Any transfer of Client Data to a Third Country shall only take place if the special requirements of Art. 44 et seq. GDPR are met.

9.2. **Transfer to Customers in countries outside of the EU/EEA.** If Controller is located in a country outside the EU/EEA and Applicable Data Protection Law requires that appropriate safeguards are put in place, the transfer of Client Data from Processor (as data exporter) to Controller (as data importer) will be subject to the EU Standard Contractual Clauses ("**EU SCC**"), which are then deemed incorporated into and form a part of this DPA, as follows: Module Four will apply; in Clause 7 the optional docking clause will not apply; in Clause 11, the option will not apply; in Clause 17, the EU SCCs will be governed by German Law; in Clause 18, disputes will be resolved before the courts of Germany; Annex I of the EU SCCs is deemed completed with the information set out in Schedule 1 to this DPA, as applicable; and subject to Section 6.1 of this DPA, Annex II of the EU SCCs is deemed completed with the information set out in Schedule 2 of this DPA.

10. MISCELLANEOUS

Priority Clause. Unless special provisions are contained in this DPA, the provisions of the Agreement shall apply. In case of any conflicts between provisions of this DPA and provisions of other agreements, in particular with the Agreement, the provisions of this DPA shall prevail.

List of Schedules:

Schedule 1: Description of the Processing

Schedule 2: Technical and Organizational Measures

Schedule 3: List of Sub-Processors

SCHEDULE 1

PARTIES TO THE PROCESSING

Relevant Information on Controller and Processor

Party:	**Customer**	**Blinks Labs GmbH**
Role	**Controller**	**Processor**
Contact person	As per agreement.	Legal Department Contact details: privacy@blinkist.com Sonnenallee 223, 12059 Berlin, for the attention of the Legal Department
UK representative (if applicable)		N/A
EU representative (if applicable)		N/A

DETAILS OF PROCESSING

Subject matter, Nature and Purpose(s) of the processing

In the framework of the Agreement, it is necessary that Blinks Labs GmbH handles Personal Data as a Processor, for which the Customer is responsible as a Controller ("**Client Data**").

Processor provides Controller with an online portal ("**Admin Space**") via which Controller can invite its own employees to Blinkist Services and/or manage their access ("**End User administration**"). In addition, the following standardized description applies:

- Collection of Personal Data via the Admin Space for the purpose of inviting End Users to the Blinkist Services.
- Access and storage of Personal Data as part of the organization and implementation of invitations.
- Use of Personal Data for the purpose of inviting End Users to the Blinkist Services.
- Deletion of Personal Data.

This DPA only relates to the data processing for the provision of the above-described Admin Space which Processor makes available to Controller.

Blinks Labs GmbH is independently responsible for all other data processing within the Blinkist Services as a separate Data Controller, as regulated in the Agreement.

Categories of Data Subjects

The categories of Data Subjects are:

Employees of the Controller who have been invited to use the Blinkist platform.

Categories of Personal Data

The transferred categories of Personal Data are: first name, last name, email address.

Special categories of Personal Data (if applicable)

Not applicable.

Frequency of the transfer

The frequency of the transfer is continuous.

Duration

Controller Personal Data will be Processed for the duration of the Agreement until deletion or return of such data as instructed by the Controller.

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL MEASURES

A. Pseudonymization measures

Measures that reduce direct references to persons during processing in such a way that it is only possible to associate data with a specific person if additional information is included. The additional information must be kept separately from the pseudonym by appropriate technical and organizational measures.

Description of the pseudonymization:

Wherever possible and appropriate, we collect, process and store data in pseudonymized form, i.e., in a form that allows an attribution to a specific person only with the aid of additional information. Access to this additional information is allocated on a need-to-know basis.

For internal and external aggregated reporting pseudonyms are dropped therefore anonymizing the data.

B. Encryption measures

Measures or operations in which a clearly legible text/information is converted into an illegible, i.e. not easily interpreted, character string (secret text) by means of an encryption method (cryptosystem).

Description of the encryption measure(s):

We use TLS (1.2) for all communication that does not use a private channel.
Data at rest is encrypted using standard block encryption algorithms.

C. Measures to ensure confidentiality

1. Physical access control

Measures that physically deny unauthorized persons access to IT systems and data processing equipment used to process personal data, as well as to confidential files and data storage media.

Description of physical access control:

Our office is protected by an electronic door lock system. Tokens to open doors are assigned to individual employees on an as needed basis and can be centrally revoked on demand at any time without access to the token. Lock access is centrally logged. There is 24/7 external security service.

Our data center providing sub-processors protect our servers against any physical access besides sub-processors maintenance staff employing industry standard data center protection techniques.

2. Logical access control

Measures to prevent unauthorized persons from processing or using data which is protected by data privacy laws.

Description of logical access control system:

We use a centrally managed SSO solution with 2FA support. The system enforces personal and individual login user credentials with strong password rules.

Access is granted on a as needed basis using a role-based rights management system.

A standardized employee on- and offboarding process is in place to ensure access rights are only granted as long as necessary and based on the role of the employee.

Production systems are completely separated from other company systems. Access to production systems align with the data access control mechanism described below.

Data at rest is encrypted.

3. Data access control

Measures to ensure that persons authorized to use data processing systems can only access personal data according to their access rights, so that data cannot be read, copied, changed or removed without authorization during processing, use and storage.

Description of data access control:

We use a role-based approach to determine access rights for all user and system combinations. Roles are based on job function and defined responsibilities using the concepts of need-to-know and least-privilege. They are assigned during the onboarding process and reviewed if the job function changes or if the employee's role changes. Role application, approval, allocation and reset are reviewed and signed off by the responsible manager. Granted roles are tied to a personal identifier and an account. Resource authorization is tied to specific roles. If the foundation for an authorization ceases to apply, the authorization/role is withdrawn.

Access to personal data via the Blinkist Platform is limited to operational personnel and restricted in the scope of access capabilities to the minimum need to fulfil operational duties.

To ensure that data cannot be read or copied by unauthorized personnel, we encrypt data in transit (HTTPS) and at rest.

D. Measures to ensure integrity

1. Data integrity

Measures to ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system.

Description of data integrity:

We employ an automated testing system for new releases which verifies the correctness of the changed component. Components that fail these tests will not be deployed to a production environment.

Changes to our main database are logged, can be audited and rolled back on a per change basis.

To ensure against unintentional data corruption the production system is segregated from other environments.

11. Transmission control

Measures to ensure that it is possible to verify and establish to which bodies personal data may be or have been transmitted or made available using data communication equipment. Data is generally only transmitted in encrypted form. Data is generally only transferred to authorized third parties (sub-processors or, if applicable, authorities that are entitled to receive information)

12. Transport control

Measures to ensure that the confidentiality and integrity of data is protected during transmission of personal data and transport of data carriers.

Description of transport control:

Personal data that is transmitted (sent and received) to or from us over public channels is encrypted (TLS 1.2). If changes to the data are detected during transmission the data is discarded and the channel is considered compromised.

13. Input control

Measures to ensure that it can be subsequently verified and ascertained whether and by whom personal data have been entered or modified in data processing systems.

Description of the input control process:

Personal data that is submitted is verified and associated with its source by a specific verification token. Interactions with our main database via the Blinkist Platform are generally verified and logged.

E. Measures to ensure availability and resilience

1. Availability control

Measures to ensure that personal data are protected against accidental destruction or loss.

Description of the availability control system:

To ensure against a loss of data all storage systems are multi-way redundant (hardware and logical). In addition, data is automatically backed up in regular intervals to physically separated systems and can be restored on demand. Backups are encrypted.

Furthermore, our data center sub-processors provide a highly available infrastructure that is secured against major physical risks by providing: alarm systems, fire alarms, air conditioning, waterproof server rooms, uninterrupted power supplies and redundant upstream connectivity.

2. Quick recovery

Measures to ensure the ability to quickly restore the availability of and access to personal data and used systems in the event of a physical or technical incident.

Description of the measures for quick recovery:

Due to the redundant storage a quick recovery is ensured.

3. Reliability

Measures to ensure that the functions of the system are available, and malfunctions are reported.

Description of measures for reliability:

All systems in our infrastructure are monitored with the help of a software-based system. In case of a malfunction our personnel follow a standardized incident management & communication process which clearly defines steps and responsibilities.

F. Measures for the regular testing and evaluation of the security of data processing

1. Verification process

Measures to ensure that the data are processed securely and in compliance with data protection regulations.

Description of verification process:

A regular internal audit by our legal department and external Data Protection Officer ensures compliance.

Our personnel are regularly trained regarding data protection and security best practices.

SCHEDULE 3

LIST OF SUB-PROCESSORS

Name and address of Sub-Processors	Services performed by the Sub-Processors	Country(ies) where the personal data is transferred to (e.g. copy of personal data is sent to that country or made remotely accessible)	Categories of Personal Data	If Personal Data is transferred outside of the EEA: Transfer mechanism used under the GDPR
Amazon Web Services EMEA SARL 39 Avenue John F. Kennedy, L-1855 Luxembourg	Cloud storage for customer Admin Space	Servers are based in the USA	First name, last name, email address, company / Name of employer	EU SCC
Auth0 10800 NE 8th Street, Ste. 600 Bellevue, WA, 98004 United States	Identity and access management services to enable single-sign-on for the login to the Admin Space. Auth0 will only receive information from customers for whom Single Sign On has been configured (upon request).	USA	First name, last name, email address, employee ID, IP addresses	EU SCC
Braze, Inc. 318 West 39th Street, New York, NY 10018 USA	Email platform for emails related to the use of Blinkist Services including user management.	USA	First name, last name, email address	EU SCC

Go1 Group Sub-processors

Blinkist is part of the Go1 Group. Personal data may be transferred to other companies within this group of companies to simplify administrative processes and to provide Blinkist's customers with even better support.

Name and address of Go1 Group Sub-Processors	Services performed by the Go1 Group Sub-Processors	Countries where the personal data is transferred to (e.g. copy of personal data is sent to that country or made remotely accessible)	Categories of personal data	If personal data is transferred outside of the EEA: Transfer tool used under the GDPR
Go1 Pty Limited 2908 Logan Road, Underwood, Queensland, Australia, 4119	Support services	Australia	All personal data stored on the Blinkist Services or submitted to Blinkist in a support request including: First name, last name, email address, name of employer	EU SCC
Go1 USA LLC 8 The Green, STE R Dover 19901, USA	Support services	USA	All personal data stored on the Blinkist Services or submitted to Blinkist in a support request including: First name, last name, email address, name of employer	EU SCC
Go1 UK Learning Limited 1st Floor West Davidson House, Forbury Square, Reading, Berkshire, RG1 3EU	Support services	Vietnam	All personal data stored on the Blinkist Services or submitted to Blinkist in a support request including: First name, last name, email	Adequacy Decision

			address, name of employer	
GO1 Vietnam Company Limited No. 271/9, Nguyen Trong Tuyen Street, Ward 10, Phu Nhuan District, Ho Chi Minh City	Support services	Vietnam	All personal data stored on the Blinkist Services or submitted to Blinkist in a support request including: First name, last name, email address, name of employer	EU SCC
Go1 Singapore PTE. LTD 7 Straits View #12-00, Marina One East Tower, Singapore (018936)	Support services	Singapore	All personal data stored on the Blinkist Services or submitted to Blinkist in a support request including: First name, last name, email address, name of employer	EU SCC
GO1 Learning (M) SDN BHD Level 25, NAZA Tower 10, Persiaran KLCC, 50088 Kuala Lumpur	Support services	Malaysia	All personal data stored on the Blinkist Services or submitted to Blinkist in a support request including: First name, last name, email address, name of employer	EU SCC