Last revised: ~~10 December 2020~~27 September 2021

EXHIBIT B: DATA PROCESSING ADDENDUM

This Data Processing Addendum (“DPA”) is an agreement between Ably and the entity that has agreed to the Ably Terms of Service (or “you” as defined in the Terms; hereinafter, “Customer”). This DPA incorporates, ~~if~~as applicable, the Standard Contractual Clauses and supplements the Ably Terms of Service (hereinafter, the "Agreement”). Capitalized terms not otherwise defined herein will have the meanings given to them in the Agreement.

Customer acknowledges that Ably is a conduit of Content transmitted through the use of the Ably Solution, some of which may, unbeknownst to Ably, contain ~~End User~~ Personal Data as defined below. Such ~~End User~~ Personal Data is held only for as long as needed to transmit it (except if and to the extent the Customer elects to store such data, as data controller). Ably does not, in the provision of the Ably Solution, otherwise use, modify, access, store, process or transmit ~~End User~~ Personal Data or even have knowledge of its existence.

Customer may be the controller of Personal Data, or the processor of Personal Data. When Customer is the controller and shares Personal Data with Ably, Ably will be the processor of the Personal Data. When Customer is the processor and shares Personal Data with Ably, Ably will be the sub-processor of the Personal Data.

This DPA applies only to the extent that Ably processes Personal Data for Customer as Customer’s processor or sub-processor.

DEFINITIONS

~~A.~~

A. In this DPA, the following definitions apply:

~~**"Data Protection Law"**~~

~~means all applicable current data protection, privacy and electronic marketing legislation, including (i) the General Data Protection Regulation (EU 2016/679) (“GDPR”) and (ii) any national implementing laws (including laws implementing the Privacy and Electronic Communications Directive 2002/58/EC) and the UK Data Protection Act 2018, regulations and secondary legislation, as amended or updated from time to time, as applicable to either party.~~

~~**"Personal Data"**~~

~~means personal data that is uploaded to, generated by or transmitted via the Ably Solution under Customer’s Ably accounts for processing as described herein.~~

~~**"Standard Contractual Clauses"**~~

~~means the standard contractual clauses for the transfer of personal data from controllers within the EEA to processors established in third countries under Directive 95/46/EC pursuant to the European Commission Decision of 5 February 2010 and located at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087 and any modifications and replacements to them or other standard contractual clauses adopted by the European Commission and entered into by the parties, from time to time.~~

~~**"sub-processor"**~~

~~means any processor that is engaged by a party to assist in its processing of Personal Data for another party.~~

~~B.~~

"Data Protection Law" means all applicable current data protection, privacy and electronic marketing legislation, including (i) the General Data Protection Regulation (EU 2016/679) ("**EU GDPR**") and (ii) any national implementing laws (including laws implementing the Privacy and Electronic Communications Directive 2002/58/EC), and the UK Data Protection Act 2018, regulations and secondary legislation, as amended or updated from time to time, as applicable to either party.

"GDPR" means the EU GDPR and/or UK GDPR, as applicable.

"Personal Data" means personal data that is uploaded to, generated by or transmitted via the Ably Solution under Customer's Ably accounts for processing as described herein.

"Standard Contractual Clauses" means the EU Standard Contractual Clauses and/or the UK Standard Contractual Clauses, as applicable.

"EU Standard Contractual Clauses" means the annex found in the European Commission decision of 4 June 2021 on the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, specifically Module 2 and Module 3 (as applicable), and any modifications and replacements to them or other standard contractual clauses adopted by the European Commission and entered into by the parties, from time to time.

"sub-processor" means any processor that is engaged by a party to assist in its processing of Personal Data for another party.

"UK GDPR" has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

"UK Standard Contractual Clauses" means the annex found in the European Commission decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, available at https://op.europa.eu/en/publication-detail/-/publication/473b885b-31d6-4f3b-a10f-01152e62be6e/ as adapted for the UK or such alternative contractual arrangement or clauses approved by the Information Commissioner's Office from time to time.

B. The terms “controller”, “data subject”, “personal data”, “processor” and “processing” will have the meanings given to them in the ~~Data Protection Law~~UK GDPR or the EU GDPR, as applicable.

DATA PROTECTION

1. Both parties will comply with all applicable requirements of Data Protection Law. This DPA is in addition to, and does not relieve, remove or replace, a party’s obligations under Data Protection Law.

2. With regards to the Personal Data, and except as provided in section 8 below, the parties agree that Ably will act as processor or sub-processor of Customer, who may act either as controller with respect to Personal Data or, where it is processing such data under the instructions and on behalf of a third party (for example, Customer’s customers) a processor.

3. Details of Personal Data processing~~:~~ (Annex 1 and Annex 2 to the EU Standard Contractual Clauses and/or Appendix 1 and Appendix 2 to the UK Standard Contractual Clauses, as applicable):

~~o~~ *Data Exporter*:~~-~~ the Data Exporter is the Customer sending Personal Data to Ably.

~~o~~ *Data Importer*:~~-~~ the Data Importer is Ably, a conduit of Content transmitted through the use of the Ably Solution, some of which may, unbeknownst to Ably, contain ~~End User~~ Personal Data.

~~o~~ *Subject matter:*~~-~~ the subject matter of the data processing under this DPA is the data and content as described below.

~~o~~ *Purpose:*~~-~~ the purpose of the data processing under this DPA is the provision of the Ably Solution initiated by Customer from time to time.

~~o~~ *Nature of the processing*:~~-~~ provision of services as described in the Agreement and initiated by Customer from time to time.

~~o~~ *Categories of data subjects:*~~-~~ the data subjects may include ~~Customer’s~~ customers, employees, guests, invitees, suppliers and End Users~~,~~ of Customer and its customers, as well as any other individuals identified or identifiable within the personal data shared by such persons.

~~o~~ *Types of Personal Data:*~~-~~ in addition to ~~End User~~ Personal Data incidentally captured in Content (“**Captured Personal Data**”), Ably collects and processes the following as a necessary step in providing the Ably Solution, all or some of which may or may not be personally identifying or identifiable information:

- ~~▪~~● IP addresses
- ~~▪~~● End User login credentials
- ~~▪~~● client device descriptions/identifiers (via Ably push notification APIs (https://www.ably.com/documentation/realtime/push)

~~o~~ *Special Categories of Data:*~~-~~ the parties do not actively or knowingly collect or process, or anticipate the transfer of special categories of ~~data~~personal data, but such data may be included in Captured Personal Data.

Processing operations:~~-~~ as described in this DPA, including Annex 1.

~~o~~

~~o~~ *Duration of processing:*

- ~~▪~~● Captured Personal Data: held by Ably momentarily (typically 2 minutes or less but up to 24 hours as necessary to provide the Ably Solution) except to the extent Customer elects to store such ~~End~~

~~User~~ Personal Data for a longer period as determined by Customer (as data controller) and via Customer's instruction to Ably, or until Customer's account is deleted.

- IP addresses: up to 14 calendar days or until Customer's account is deleted.
- End User login credentials: up to 14 calendar days or until Customer's account is deleted.
- client device descriptions/identifiers: until Customer's account is deleted. Customer agrees to delete such data as soon as it is no longer needed.

Competent Supervisory Authority: Data Protection Commissioner of Ireland (EU); Information Commissioner's Office (UK).

4. Customer will ensure and warrants that it has all necessary appropriate consents and notices, in any form required by Data Protection Law or by other laws of the UK or the European Union~~,~~ (as applicable), in place to enable lawful transfer of the Personal Data to Ably for the duration and purposes of the Agreement.

5. Customer will ensure and warrants that ~~where~~, for Personal Data ~~is~~ transferred ~~outside~~from the European Economic Area ("EEA") to anywhere outside the EEA, or from the UK to anywhere outside the UK, as part of Customer's use or deployment of the Ably Solution, and such transfer is not to a third country that the Commission considers to provide an adequate level of protection (in the case of transfers subject to EU GDPR) or that the UK Secretary of State considers to provide an adequate level of protection (in the case of transfers subject to UK GDPR), adequate measures will be taken to ensure the Personal Data will be protected to an adequate level and the data subjects' rights under the Data Protection Law will not be prejudiced by such a transfer. Subject to Ably's obligation in section 9.5 below with respect to Ably sub-processors, and section 11 below with respect to the Standard Contractual Clauses, Customer acknowledges that Customer is solely responsible for ensuring that Personal Data is transferred out of the EEA or the UK in full compliance with the Data Protection Law.

~~5.~~

6. Customer confirms that it has assessed any security measures in place at the time of this Agreement, and that it will continue to do so on an ongoing basis to ensure its obligations under this DPA. Customer is solely responsible (as between the parties and to data subjects and supervisory authorities) if such measures fail to meet the standards required by Data Protection Law ~~standard.~~.

~~6.~~

7. Customer undertakes and confirms that any information required to be provided to a data subject has been so provided or an applicable exemption is available and is being relied upon by Customer.

8. Customer and Ably agree that to the extent they process any personal data of the other's personnel in connection with their entry into the Agreement or the management of their business relationship, they process such data as independent controllers.

9. Ably shall, in relation to any Personal Data processed in connection with the provision of the Ably Service:

~~o~~9.1. process that Personal Data only on the written instructions of Customer except to the extent Ably is required to process data by applicable law. Where Ably is relying on applicable law as the basis for processing Personal Data, Ably shall without undue delay notify Customer unless applicable law prohibits Ably from so notifying Customer;

9.2. not access or use, or disclose to any third party, any Personal Data, except, in each case, as necessary to maintain or provide the Ably Solution, or as necessary to comply with the law or a valid and binding order of a governmental body or court;

~~o~~

~~o~~9.3. ensure that it has in place appropriate technical and organisational measures set forth in Annex 1 to this DPA to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures;

~~o~~9.4. ensure that all Ably personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential;

~~o~~9.5. ensure that where sub-processors are used outside the EEA or the UK such that Personal Data is transferred from within the EEA to anywhere outside the EEA~~,~~ or from the UK to anywhere outside of the UK, and such transfer is not to a third country that the Commission considers to provide an adequate level of protection (in the case of transfers subject to EU GDPR) or that the UK Secretary of State considers to provide an adequate level of protection (in the case of transfers subject to UK GDPR), adequate measures will be taken to ensure the Personal Data will be protected to an adequate level and the data subjects' rights under the Data Protection Law will not be prejudiced by such a transfer;

~~o~~9.6. maintain records of processing activities carried out on behalf of Customer as required by Data Protection Law;

~~o~~9.7. taking into account the nature of the processing, assist the Customer, in so far as this is possible, in responding to any request from a data subject and in ensuring compliance with its obligations under Data Protection Law with respect to security, breach notifications, data protection impact assessments and consultations with supervisory authorities or regulators;

~~o~~9.8. notify Customer without undue delay on becoming aware of a security incident affecting Personal Data. Ably is not obligated to report incidents that result in no unlawful or accidental destruction, loss, alteration, disclosure of, or access to Personal Data or to any of Ably's equipment or facilities storing Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents. Ably's obligation to report or respond to a security incident under this section is not and will not be construed as an acknowledgement by Ably of any fault or liability of Ably with respect to the incident;

9.9. make available to Customer all information reasonably necessary to demonstrate compliance with the obligations in this section 9; and

~~o~~

~~o~~9.10. at the written direction of Customer, delete Personal Data on termination of the Agreement unless required by applicable law to store the Personal Data.

10. Customer will immediately notify Ably if any necessary appropriate consents and notices required to enable lawful transfer of Personal Data to Ably for the duration and purposes of this Agreement have been breached, terminated, withdrawn or are otherwise no longer valid.

11. The parties agree that the Standard Contractual Clauses apply if Personal Data is transferred to Ably or its sub-processors located in a country that is outside of the EEA~~.~~ or the UK and such transfer is not to a third country that the Commission considers to provide an adequate level of protection (in the case of transfers subject to EU GDPR) or that the Secretary of State considers to provide an adequate level of protection (in the case of transfers subject to UK GDPR). As used in this section, the terms "Data Importer" and "Data Exporter" will have the meanings given to them in the Standard Contractual Clauses. The parties acknowledge that for the purposes of the Standard Contractual Clauses Ably is acting in the capacity of a Data Importer and Customer is the Data Exporter (notwithstanding that Customer may be located outside of the EEA or the UK or is acting as a processor on behalf of third~~-~~-party controllers). Each party will comply with the applicable obligations of the Standard Contractual Clauses in their respective roles as Data Exporter and Data Importer. The data subjects, categories of data, and processing operations (as required to be disclosed in Appendix 1 of the Standard Contractual Clauses) are as set forth in this DPA. Annex 1 to this DPA details the technical and security measures Ably has implemented, as required to be disclosed in Appendix 2 of the Standard Contractual Clauses.

12. The parties further agree that the governing law of the Standard Contractual Clauses entered into by Ably and the Customer will be as follows: where the ~~governing law of the country in which Customer is established, if~~EU Standard Contractual Clauses apply and the Customer is established in the EEA~~. If Customer is not established in the EEA~~, the laws of ~~the country within the EEA in which the initial data exporter is established will apply~~Ireland control; and where the UK Standard Contractual Clauses apply, the laws of England and Wales control. If any inconsistency arises between this section 12 and any other provision for the governing law of the Standard Contractual Clauses entered into between Customer and Ably, this section 12 will take precedence.

13. Customer acknowledges and agrees that it shall exercise its audit rights under this DPA (including where applicable, the Standard Contractual Clauses) and any audit rights granted by Data Protection ~~Laws~~Law, by instructing Ably to comply with the audit measures described in section (e) of Annex 1 to this DPA.

14. Ably represents and warrants that it has not received any order, request or other communication from a governmental body for the disclosure of personal data and it shall:

~~o~~14.1. if it receives such order, request or other communication, attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, Ably may provide Customer's basic contact information to the relevant body. If compelled to disclose Customer Data to a governmental body, then Ably will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Ably is legally prohibited from doing so;

~~o~~14.2. publish a transparency report or provide information to Customer on request regarding: (a) the number of orders, requests or other communications from governmental bodies for the disclosure of personal data and/or assistance in surveillance processes and the type of information requested, (b) its responses to the foregoing, and (c) its process for challenging such confidential and non-confidential orders, requests and communications; and

~~o~~14.3. notify Customer if its ability to maintain the confidentiality and security of personal data has been compromised for any reason including by orders, requests or communications described above, and cease processing, including receiving such personal data.

15. Customer agrees that Ably may use sub-processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support services, and consents to the use of sub-processors as described in this section. The Ably website (currently posted at https://ably.com/legals/sub-processors/) lists sub-processors that are currently engaged by Ably to deliver the Ably Service. At least 10 business days before Ably engages any new sub-processor to carry out processing activities on Personal Data on behalf of Customer, Ably will update the applicable website and provide Customer notice of that update as per the means specified for notices in the Agreement (sec. 2.12). If Customer objects to a new sub-processor, Customer must notify Ably in writing within ten days of Customer's notice of the updated website (without prejudice to any termination rights Customer has under the Agreement~~).~~), after which time Customer shall be deemed to have consented to the new sub-processor's appointment.

~~15.~~

16. California Consumer Privacy Act (CCPA) Notice: as a "Service Provider" (as that term is defined in the CCPA), Ably will process California personal data that is subject to the CCPA strictly for the purpose of providing to Customer the solutions and services described under the Agreement, or as otherwise permitted by the CCPA, and shall not retain, use, or disclose such data for any other purpose.

17. The parties agree that, if any new versions of revisions to the EU Standard Contractual Clauses are approved by the European Commission, or the UK Standard Contractual Clauses are adopted by the UK, such that the implementation of the Standard Contractual Clauses in this DPA no longer applies or is no longer appropriate, the parties shall work together to enter into the new standard contractual clauses as appropriate.

18. Where the EU Standard Contractual Clauses apply to transfers of personal data governed by this DPA, the following options shall be deemed to be selected and incorporated, each clause reference in this section being a reference to a clause in the EU Standard Contractual Clauses:

18.1. Clause 7 shall not apply.
18.2. At Clause 9, option 2 shall apply for both Module 2 and Module 3.
18.3. At Clause 11, the optional redress mechanism shall not apply.

DPA ANNEX 1: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES (Annex II/Appendix 2 to the Standard Contractual Clauses as applicable)

~~1.~~ a) Access Control

~~1.~~ i) Preventing Unauthorized Product Access

Outsourced processing: Ably hosts its Service with ~~Amazon Web Services Inc~~AWS and/or applicable affiliates. Additionally, Ably maintains contractual relationships with vendors in order to provide the Service. Ably relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: Ably hosts its product infrastructure with multi-tenant, outsourced infrastructure provider Amazon Web Services Inc. The physical and environmental security controls are audited for SOC 2 Type ~~2~~II (~~https://aws.amazon.com/compliance/soc-faqs/~~https://aws.amazon.com/compliance/soc-faqs/) and ISO 27001 (https://aws.amazon.com/compliance/iso-27001-faqs/) compliance, among other certifications.

Authentication:~~-~~ Ably has implemented a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization:~~-~~ Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Ably's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access:~~-~~ Public product APIs may be accessed using an API key.

~~2.~~ ii) Preventing Unauthorized Product Use

Ably implements industry standard access controls capabilities for the internal networks that support its products.
Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: Ably has implemented a Web Application Firewall (WAF) solution to protect internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in Ably's source code repositories is performed, checking for identifiable software flaws and known vulnerabilities.

Penetration testing: Ably maintains relationships with industry recognized penetration testing service providers for regular penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

~~3.~~ iii) Limitations of Privilege & Authorization Requirements

Product access:~~-~~ A subset of Ably's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through “just in time” requests for access; all such requests are logged.

Staff:~~-~~ All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

~~2.~~ b) Transmission Control

In-transit:~~-~~ Ably makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces. Ably’s HTTPS implementation uses industry standard algorithms and certificates.

At-rest:~~-~~ Ably stores user passwords following policies that follow industry standard practices for security, and ensure that all passwords are never stored in plain text formats.

~~3.~~ c) Input Control

Detection:~~-~~ Ably designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Ably personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking:~~-~~ Ably maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Ably will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication:~~-~~ If Ably becomes aware of unlawful access to Customer data stored within its products, Ably will: 1) As a member of the ICO in the UK, notify them and follow their guidelines in regards to procedure; 2) notify the affected Customers of the incident if permitted under applicable law; 3) provide a description of the steps Ably is taking to resolve the incident; and 4) provide status updates to the Customer contact, as Ably deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer’s contacts in a form Ably selects, which may include via email or telephone.

~~4.~~ d) Availability Control

Infrastructure availability:~~-~~ The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. As Ably’s service is designed to be available across many regions simultaneously, the availability offered is much higher than the underlying infrastructure provider in any single region. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance:~~-~~ Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups:~~-~~ Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

Ably’s products are designed to ensure redundancy and continuity in spite of failures. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists Ably operations in maintaining and updating the product applications and backend without downtime.

e) Transparency

~~5.~~

Customer acknowledges that Ably is regularly audited by independent third party auditors and internal auditors respectively. Upon written request, Ably shall supply (on a confidential basis) a summary copy of its most current audit report(s) to Customer. In addition, Ably shall respond to all reasonable requests for information made by Customer to confirm Ably's compliance with this DPA, by making additional information available regarding its information security program upon Customer's written request, provided that Customer shall not exercise this right more than once per calendar year.

f) Back Doors

~~6.~~

Ably has not purposefully created back doors or similar programming that could be used to access the system and/or personal data. Ably has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems.