Data Processing Addendum (as of May 20, 2024)

This Data Processing Addendum (**"DPA"**) constitute a part of Airbridge Service Agreement including any order forms, exhibits, appendices, annexes, terms or policies attached to it(collectively **"Agreement"**), entered into by and between Customer and AB180 Inc.(hereinafter referred to as "Company") that governs Customer's use and Company's provision of Services.

1. Definitions
   In this DPA, capitalized terms not otherwise defined hereunder shall have the meaning given to them in the Agreement.
   a. "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "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
   b. "CCPA" means the California Consumer Privacy Act and its amendments including the California Privacy Rights Act ("CPRA").
   c. "Controller" means the person or entity that determines the purposes and means of the processing of Personal Data or otherwise is in charge of making decisions regarding the processing of Personal Data, including equivalent terms under Data Protection Laws and Regulations such as "Business".
   d. "Data Protection Laws and Regulations" means all laws and regulations applicable to a party in its use or provision of the Services, in connection with the processing of Personal Data pursuant to the Agreement, including GDPR, UK GDPR, and CCPA.
   e. "Data Subject" means the identified or identifiable person to whom Personal Data Relates, including equivalent terms under Data Protection Laws and Regulations such as "Consumer".
   f. "Data Subject Right" means any right afforded to a Data Subject under Data Protection Laws and Regulations.
   g. "GDPR" means European Union(EU) General Data Protection Regulation, a regulation on personal data protection (Regulation 2016/679), which came into full effect on May 25, 2018.
   h. "Personal Data" means any information that relates to an identified or identifiable natural person and is protected under Data Protection Laws and Regulations such as "Personal Information", where such data is Customer Data processed by the Company in the provision of its Services pursuant to the Agreement.
   i. "Processing" means any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
   j. "Processor" means a person or entity which Processes Personal Data on behalf of the Controller, including equivalent terms under Data Protection Laws and Regulations such as "Service Provider".
   k. "Personal 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 by the Company or its Sub-processors which Company becomes aware of.

l. "Sub-processor" means any processor engaged by the Company or its Affiliates engaged in Processing of Personal Data.
m. "UK GDPR" means the UK's General Data Protection Regulation and other applicable data protection laws of the UK.
n. "Standard Contractual Clauses" means the Standard Contractual Clauses for transfers of Personal Data to third countries, as approved by the European Commission by implementing decision 2021/914 of 4 June 2021.
o. "UK Addendum" means the template International Data Transfer Addendum issued by the UK Information Commissioner's Office under section 119A of the Data Protection Act 2018 (as updated from time to time).

2. Processing of Personal Data
    a. With respect to Processing of Personal Data, the parties acknowledge and agree on that Customer is the Controller and Company is the Processor. Company shall not Process Personal Data other than for the purpose of provision of Services or out of the instructions specified in the Agreement or in this DPA, including the instructions reasonably requested or guided by the Customer in a written form, unless such Processing is required by applicable laws to which the Company is subject; in such a case Company shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
    b. Customer warrants and represents that its instructions to Process Personal Data comply with the Data Protection Laws. Customer shall be solely responsible for the accuracy and legality of the Personal Data and ensure it has appropriate legal rights to enable the Processing of Personal Data pursuant to the Agreement and this DPA. Customer specifically warrants that its use of the Services shall not violate the rights of any Data Subject.
    c. Annex 1 sets forth the details of the Processing of Personal Data. In no event shall Customer configure the Services to collect or cause Company to Process Personal Data that is beyond the scope set forth in Annex 1, including any Restricted Data as defined in the Agreement.
    d. Company shall not sell or share Personal Data and will notify the Customer if Company is no longer able to remain compliant to Data Protection Laws and Regulations.

3. Rights of Data Subjects
    a. Customer shall be solely responsible for complying with any statutory obligations concerning requests to exercise Data Subject rights under Data Protection Laws including but not limited to for access, rectification or deletion of Personal Data.
    b. Company shall comply with the following:
        i. Unless prohibited by any applicable laws, Company shall promptly notify Customer of all requests from Data Subject, if received any, under any Data Protection Law in respect of Personal Data.
        ii. Company shall not respond to any request except on the written instructions of the Customer or as required by any applicable laws.

4. Personal Data Breach

a. Company shall promptly notify Customer upon the Company becoming aware of any Personal Data Breach that may affect the Customer. In such events, Company shall provide Customer with any relevant information to assist Customer to meet any obligations to inform Data Subjects or any relevant authorities of Personal Data Breach under Data Protection Laws.
b. Company shall do its best efforts and take all necessary steps to remediate and mitigate the impact of each Personal Data Breach, at its sole discretion and expense, except for the cases or to the extent caused by the Customer. To the extent the Customer requests the Company to conduct any additional steps or measures, any such steps or measures agreed with the Company at its sole discretion shall be executed at the Customer's sole expense.

5. Personnel
Company shall take all reasonable steps to ensure that access to Personal Data is limited on a need to know basis and that all the Company personnel receiving such access are subject to confidentiality obligations regarding their access to or use of the Personal Data.

6. Security
Company shall implement appropriate technical and organizational measures to ensure an appropriate security, including protection against Personal Data Breach, confidentiality and integrity of Personal Data, as set forth in [Annex 2].

7. Return and Deletion of Personal Data
At the termination of the Agreement, Company shall return Personal Data by enabling Customer to export its Personal Data as set forth in applicable Data Protection Laws. Company shall provide a certificate of deletion once Personal Data has been deleted from the Services upon request from the Customer, provided that Personal data related to the Customer shall be completely deleted 30 days after the termination of the Agreement.

8. Sub-processors
    a. Customer acknowledges that Company's Affiliates may be retained as Sub-processors, and also authorizes Company and its Affiliates to respectively appoint Sub-processors in accordance with this Section 8 and regarding terms in the Agreement.
    b. Attached hereto as [Annex 3] is a current list of Sub-processors for the Services. The list is subject to changes and the updated list shall be notified to the Customer on the Company's website.
    c. Customer may object to the Company's use of a new Sub-processor(s) by notifying Company promptly in writing within ten (10) business days after the Company's notification in accordance with Section 8.b. If Customer notifies Company of any reasonable objections in relation to the notified new Sub-processor(s), Company shall not utilize corresponding Sub-Processor(s) to Process Personal Data until reasonable steps have been taken to address the objection raised by the Customer, such as a change to the Customer's configuration or use of the Services to avoid Processing of Personal Data by the corresponding Sub-Processor(s). In case such steps taken by the Company are not sufficient to resolve Customer's objections and it cannot be resolved within thirty (30) days from the date of the objection notified to the Company, then parties may terminate the Agreement immediately by written notice to the other party to the extent that it relates

to the Services which require the use of the objected Sub-Processor, without bearing liability for such termination.

d. With respect to the listed Sub-processors (including new Sub-processors updated within the term of the Agreement), Company shall comply with the following.
    i. Company shall take all reasonable steps to ensure that each Sub-processor is committed to provide the level of protection for Personal Data required by the Agreement.
    ii. Company shall ensure that the arrangement between the Company and each Sub-processor is governed by a written agreement, including terms which, to the extent applicable to the nature of services provided by the Sub-processor, offer a level of protection that, in all material respects, are consistent with the levels set forth in this DPA and the Agreement.
    iii. Company shall remain fully liable to the Customer for the performance of each Sub-processor's data protection obligations where the Sub-processor fails to fulfill such obligations.

9. Data Protection Impact Assessment and Prior Consultation
   At the written request of the Customer, Company and each Affiliate shall provide reasonable assistance to the Customer, at Customer's expense, with any data protection impact assessments or prior consultations with appropriate authorities, as required under any applicable Data Protection Laws. Such assistance shall be solely in relation to Processing of Personal Data by the Company.

10. Limitation of Liability
    Each party's and all of its Affiliates and Sub-processor's liability, taken together in the aggregate, arising out of or related to this DPA is subject to the Agreement and Terms of Service referenced to it. Any reference in such to the liability of a party means the aggregate liability of that party and all of its Affiliates and Sub-processors under the Agreement and all DPAs together.

11. Audit
    a. Company shall provide Customer with information that is necessary to demonstrate compliance with this DPA on the Customer's request, and shall allow for and contribute to audits by an authorized auditor mandated by the Customer in relation to the Processing of Personal Data by the Company and its Affiliates.
    b. To the extent Company has undergone a third party independent audit based on SOC 2 Type II or similar standards, then any audit right arising pursuant to this DPA shall be first satisfied by providing Customer with a summary of the report of such audit. If Customer is not satisfied by the third party audit report for a reasonable basis, then Customer may request that an authorized auditor perform an audit pursuant to Section 11.a. and subject to Section 11.3.
    c. Customer shall give Company with a written notice at least ten (10) business days prior to any audit to be conducted under this Section, and shall use its best efforts to efforts to avoid causing any damage, injury, or disruption to the Company's premises, equipments, personnel and business while its personnel or agents are are on those premises in the course of such audit. All such audits shall be subject to the confidentiality obligations set forth in the Agreement. Customer and Company shall mutually agree upon the scope, timing and duration of the Audit in addition to any reimbursement of expenses for which

Customer shall be responsible. Any such audit shall not take place more than once a year, except where required by Data Protection Laws or due to a Personal Data Breach. Notwithstanding the foregoing, Company has no obligation to cooperate with such audits in case the audit is conducted outside the Company's business hours or is related to the Company's competitors. Customer shall share a full audit report with the Company and shall not share it with any third party except for its legal attorneys who are bound to confidentiality. Customer shall not use such report for any purpose other than to assess Company's compliance with this DPA.

12. Data Transfers
    Customer acknowledges that Company may transfer and Process Personal Data outside of the country which it originated in order to perform the Services for the Customer including to such countries identified in [Annex 3] and Sub-processors' websites. Customer shall ensure that it obtains any necessary consents or has the necessary rights to authorize such transfer. Subject to the foregoing, Company shall only make such transfers in compliance with Data Protection Laws.

13. International Transfer of Personal Data
    For Personal Data transfers to non-EU/EEA countries, for which no adequacy decision according to Art. 45 of the GDPR ("Third Countries"), Company shall comply with the Standard Contractual Clauses or the UK Addendum. In the event of a conflict between this DPA and the Standard Contractual Clauses or the UK Addendum, the terms in the Standard Contractual Clauses or the UK Addendum shall take precedence.

[Annex 1] Details of Processing
[Annex 2] Security Measures for Company
[Annex 3] Sub-processors

Date:

"Customer"	**"Company"**
Company Name	AB180 Inc.
Business Registration No.	550-88-00196
Company Address	3-4F, 17, Gangnam-daero 61-gil, Seocho-gu, Seoul, South Korea (06619)
Name of Representative	Sung Pil Nam
Title of Representative	CEO
Signature:	Signature:

[Annex 1] Details of Processing (as of May 20, 2024)

1. **Nature and Purpose of Processing**

   Company will Process Personal Data as necessary to perform its Services pursuant to the Agreement, as further described in Terms of Service(https://www.airbridge.io/terms-of-service) and the Documentation, and as further instructed by the Customer in its use of the Services. The Services offered by the Company are based on a software-as-a-service platform that includes measurement and analytics services, as is further described in the Agreement and the Documentation.

2. **Duration of Processing and Data Retention**

   The duration of Processing Personal Data shall be for the term of the Agreement unless Customer requests data export or deletion upon Section 7 of this DPA. Notwithstanding the above, if the term of the Agreement extends beyond five years, the processed personal information will still be retained for a maximum of five years from the time it was processed.

3. **Categories of Data Subjects**

   Customer may submit the following data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion:
   (i) Personal Data of End Users
   (ii) Personal Data of prospective or former End Users

4. **Type of Personal Data**

   Customer may submit Personal Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and thich may include, but is not limited to the following categories of Personal Data:
   (i) Email address
   (ii) Device data
   (iii) ID data(e.g. IDFA, ADID, GAID, etc.)

   For clarity, Customer shall not configure the Services to collect any Restricted Data defined in the Terms of Service.

[Annex 2] Security Measures for Company (as of May 20, 2024)

The goal of this document is to provide Customer with a detailed overview of the operational activities that Company undertakes to keep Customer's data secure. If this document does not fully address the needs or if there are additional questions, please contact compliance@ab180.co and we will respond promptly.

1. **Compliance and Certifications**
   - Company has implemented managerial and technical measures as mandated by Data Protection Laws and Regulations to ensure the protection of Personal Data.
   - In addition, Company's information security management system undergoes annual audits by a recognized independent auditing organization to maintain the following certifications

Name	Validity period	Certification body
ISMS	Oct 04, 2023 ~ Oct 03, 2026	Korea Internet & Security Agency(KISA)
ISO/IEC 27001:2013	Jun 27, 2023 ~ Oct 31, 2025	SGS Korea
ISO/IEC 27017:2015	Sep 04, 2023 ~ Sep 04, 2026	SGS Korea
ISO/IEC 27018:2019	Sep 04, 2023 ~ Sep 04, 2026	SGS Korea

2. **Organization**
   - Company has a dedicated Information Security Team.
   - An Information Security Committee comprised of executive and engineering leads periodically reviews and approves the plans and results of our security activities.

3. **Security Policy, Guidelines and Manuals**
   - Company has established and published information security policies, guidelines, and manuals that are readily available to all Company employees.
   - The policies, guidelines, and manuals are reviewed and revised at least annually by the Information Security Team.

4. **Information Asset and Risk Management**
   - Identified and managed are all information assets (servers, databases, networks, etc.) that are required to operate Company.
   - Periodic risk assessments are conducted to determine the likelihood and impact of vulnerabilities based on the criticality of the asset and derive a risk rating based on that.

5. **Internal Audit and Penetration Testing**
   - Company conducts periodic checks and internal audits of high service impact systems and logs and report to the CISO.
   - Company conducts periodic pentesting through a reputable security organization to identify and remediate vulnerabilities.

- When outsourcing development, infrastructure maintenance, or Personal Data processing to external parties, Company thoroughly audits their compliance with established security and privacy processes.

6. **Infrastructure and Physical Security**
   - Company is serviced by Amazon Web Services ("AWS") in the Tokyo Region and does not operate its own data centers, physical servers, routers, or load balancers.
   - Physical and environmental security is based on a ‘Shared Responsibility Model’ between AWS and Company, and the location of physical equipment is not disclosed in accordance with AWS's security policy.
   - Company operates in two or more Availability Zones to increase the effectiveness of business continuity and disaster recovery.

7. **Data Encryption, Backups and Logging**
   - Customer data is located in Japan (AWS Tokyo Region)
   - Sensitive data is stored, at rest, encrypted using AWS SSE-S3 (AES-256).
   - In transit, data that is sent and received is encrypted with TLS 1.2 or higher protocols.
   - All decryption and access to data is recorded in audit logs.
   - Critical infrastructure such as load balancers and servers are redundant, and data is backed up regularly to prevent loss.

8. **Access Control Policy**
   - All employees have only the minimum privileges necessary for the purpose of their work, approved by the lead of the organization.
   - All authorization and permission logs are kept and managed, with their contents regularly reviewed and assessed (Account Review) and approved by the CISO.
   - Moreover, Company provides a service access permission management feature (Dashboard) to ensure safe utilization of the service by customers. For further details on the access permission management functionality, please consult the following link. (https://help.airbridge.io/en/guides/user-management)

9. **Personnel Security and Training**
   - The laptops utilized by employees are outfitted with endpoint security solutions managed by the Information Security Team, notably Data Loss Prevention (DLP) solutions aimed at detecting and thwarting data breach attempts.
   - To ensure the safe use of business systems, strong passwords are required for accessing them. Additional secure access methods or secure authentication methods are enabled whenever possible.
   - Information security training is provided for employees at least once a year. Development engineers and personal information handlers receive specialized training based on their job duties.
   - All employees (including outsourced personnel) are required to sign an information security pledge when they join the company or sign a service contract, ensuring that they are clearly aware of their information protection responsibilities.

10. Development and Maintenance

- Company utilizes tools such as GitHub to effectively manage the development lifecycle(SDLC).
- Testing is conducted only in local or testing environments.
- Source code is controlled in a private GitHub repository, and deployment to production environments is regulated to occur only after code review and approval.

11. Information Security Incident Management and Monitoring

- Amazon Inspector is utilized to periodically scan all instances for known security vulnerabilities at both the OS and application levels.
- Software and libraries with identified security vulnerabilities are patched to their latest versions, taking into account compatibility with existing systems, and all server instances are operated based on standardized OS images with system hardening, including default security settings.
- All servers are operated in AWS's Virtual Private Cloud (VPC), isolated from external networks, and unauthorized external access is prevented through various measures including Security Groups.
- Amazon GuardDuty, an intelligent threat detection tool, monitors network flow logs, DNS logs, AWS console access, and API call logs in real-time.
- In the event of threat detection, PagerDuty alerts the Information Security Manager for prompt action, and regular simulated training and evaluations are conducted to prepare for actual security incidents.

12. Business Continuity Management and Disaster Recovery

- All systems and components included in the data pipelines within the infrastructure are monitored 24/7/365 to minimize damage and facilitate rapid recovery in the event of incidents or outages.
- Utilizing third-party tools such as PagerDuty, incidents are managed on a ticket basis, enabling engineers to swiftly address issues and minimize service impact.
- Regular simulated training exercises are conducted to prepare for disaster recovery scenarios. Through training, relevant personnel are thoroughly familiarized with disaster response manuals to prepare for actual incidents.
- Customers can check the system status and scheduled system maintenance plans at any time through the System Status page.

13. Customer Responsibilities

- Please refrain from disclosing Airbridge account information (especially passwords and token values) to external.
- After using the service on a public PC, be sure to log out and avoid sharing a single account among multiple users. If multiple users within the organization need access to the Airbridge dashboard, please utilize the administrator's user invitation feature.
- Please only invite app administrator permissions when absolutely necessary. When inviting external agencies as app administrators, customers may require them to complete documents such as security pledges according to the customer's compliance requirements.
- Please regularly delete user accounts that are no longer needed.
- Customers can utilize the Activity History feature provided by Company to prevent and detect data breaches.

- Compliance responsibility for customer data lies with the customer. Please ensure compliance with regulations to enable lawful processing of customer data by Company. Specifically, if providing services in South Korea, consent for Personal Data ‘processing' and 'overseas transfer’ of Personal Data according to the PIPA may be required. Additionally, if the Customer is a corporation established within the EU or an EU citizen, Personal Data should not be transmitted to Company without valid user consent using the SDK's Opt-Out feature.
- Company does not collect Personal Data of children under the age of 14. Customers are advised to use the SDK's Opt-Out feature to prevent the transmission of Personal Data of children under the age of 14 to Company.
- Please be aware that unauthorized Pentests, vulnerability assessments, and security audits may result in sanctions under contracts and relevant laws.

[Annex 3] Sub-processors (as of May 20, 2024)

Company utilizes Sub-processors to ensure efficient and seamless service delivery. They handle some of the processing of Customer Data on behalf of Company.

Sub-processors comply with security and privacy matters within the scope of the services they provide. Company is responsible for supervising this.

This is a list of Company's Sub-processors. However, this is a list of Sub-processors for Company's processing of Customer data in accordance with this DPA. The list of processors the Company entrusts processing of Personal Data of the Customer to provide Airbridge Dashboard (airbridge.io) services can be found separately in the Privacy Policy on the Airbridge website.

Category	Entity Name	Services Provided	Location of Processing
Storage and Analytics Services	Amazon Web Services, Inc.	Third-party hosting provider (Physical operations included)	Japan
	Snowflake Computing Inc.	Data Warehouse	Japan
Monitoring	New Relic, Inc	Monitoring the performance of the infrastructure	United States

Customer data utilized and stored by Sub-processors will be destroyed or transferred as soon as practicable in accordance with the agreement between Company and Sub-processors, and Company will closely monitor the results of such destruction or transfer.