AHI Data Processing Agreement

PARTIES

(1) **Advanced Health Intelligence Ltd** (ABN 85 602 111 115) of Unit 5, 71-73 South Perth Esplanade, South Perth Western Australia 6151 (the "Service Provider", "AHI"); and

(2) Client as defined in the Master Services Agreement under Commercial Details (the "Licensee or You").

BACKGROUND

(1) Under an agreement (the "Master Services Agreement") between AHI and the Licensee with the Contract Reference indicated in the Master Services Agreement, AHI provides to the Licensee, access to the AHI cloud platform for the purpose of providing smartphone and cloud based digital biometric processing services.

(2) The provision of the AHI Services involves the processing of Personal Data (as defined below) by AHI on behalf of the Licensee.

(3) The parties have agreed to enter into this Data Processing Agreement ("DPA") to meet the requirements of applicable Data Protection Law.

THE PARTIES AGREE as follows:

1. DEFINITIONS AND INTERPRETATION

1.1. In this DPA any capitalised expression used but not defined in this DPA shall have the meaning provided to it in the Master Services Agreement and the following expressions shall have the following meanings:

Account Data means Personal Data that relates to the Service Provider's supplier relationship with the Licensee.

Controller shall mean the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

Consent shall mean any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

Data Protection Law refers to all laws and regulations applicable to the Service Provider's processing of Personal Data under this DPA including, without limitation:

- Australian Privacy Act 1998 (Cth) ("**APA"**) and associated legislation such as, the Australian Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) ("**NDB Law"**)
- California Consumer Privacy Act, California Civil Code Sections 1798.100 et seq and its implementing regulations ("**CCPA"**)

- UK General Data Protection Regulation ("**UK GDPR"**)
- EU General Data Protection Regulation ("**EU GDPR"**)
- Brazilian General Data Protection Law ("**LGPD"**)
- Peru's Personal Data Protection Law (N°29733 ("**PDPL"**)) and its Regulation (N°003-2013-JUS-Regulation of the PDPL)
- China's Personal Information Protection Law ("**PIPL"**).
- Singapore's Personal Data Protection Act 2012 (No. 26 of 2012)
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- UAE's The Personal Data Protection Law, Federal Decree Law No. 45 of 2021
- South Africa's The Protection of Personal Information Act (PoPIA)
- Hongkong's The Personal Data (Privacy) Ordinance (Cap. 486) (Ordinance)
- Vietnam's Decree No. 13/2023/ND-CP on the Protection of Personal Data (April 17, 2023)
- New Zealand's Privacy Act 2020 ('the 2020 Act')
- The Digital Personal Data Protection Act of India (DPDP)
- Malaysia's Personal Data Protection Act 2010 ("PDPA")
- Saudi Arabia's Personal Data Protection Law
- Mexico's the Protection of Personal Data Law
- IRAQ (There is no general data protection regulation. Regulator: There is no general data protection authority. Summary: Although Iraq has not adopted a comprehensive data protection legislation applicable to private organisations, it has established a law regulating privacy within the public sector)
- Egypt's Personal Data Protection Law

Data Subject shall mean an identified or identifiable natural person to whom Personal Data relates.

End User means an individual Data Subject who is a customer or user of any Licensee product or service which incorporates the AHI Service or relies upon the AHI Platform.

End User Data means Personal Data about an End User provided to the Service Provider by the End User and/or the Licensee and including the End User's height, weight, biological sex, age, whether the End User: is a smoker, has hypertension, is on blood pressure medication,

is diabetic, together with facial blood-flow information, generated on End User devices by the AHI Services.

Licensed SDK means the software development kits listed at Schedule 1 of the Master Services Agreement.

Licensee Products means the Licensee software products listed at Schedule 1 of the Master Services Agreement.

AHI Platform means the AHI public cloud environment described at Parts A and B of Schedule 3 of this DPA.

AHI Services means smartphone digital biometric processing services provided by AHI, using the AHI Platform, to End Users through Licensee Products that integrate the Licensed SDKs.

Personal Data means any information relating to a person ('Data Subject') 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 person.

Processor shall mean a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unavailability, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

'processing' and 'process' shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Service Data means data processed by the Service Provider for the purposes of transmitting and exchanging End User Data including, without limitation, the date, time, duration, and type of communication; information collected from End User devices about how they use the AHI Service; and activity logs used to optimise and maintain the performance and security of the AHI Services and to investigate and prevent system abuse.

Sensitive Data is specific to each region's data privacy regulation e.g. Sensitive data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, or genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation; and Personal Data relating to criminal convictions and

offences and shall be deemed to include "Sensitive Information" as defined in the *Australian Privacy Act 1998* (Cth).

Silhouette means the image of an End-User represented as a solid shape or a single colour, with the interior of a silhouette being featureless.

Supervisory Authority is specific to each region's data privacy regulation e.g., Supervisory Authority means an independent public authority which is established under the UK GDPR or the EU GDPR.

3D Model means a virtual 3D representation of an End-User's human body shape.

1.2. In this DPA:

1.2.1. a reference to this DPA includes its schedules.

1.2.2. clause, paragraph, schedule, or other headings in this DPA are included for convenience only and shall have no effect on interpretation.

1.2.3. a reference to a 'party' includes that party's successors and permitted assigns.

1.2.4. words in the singular include the plural and vice versa.

1.2.5. any words that follow 'include', 'includes', 'including', 'in particular' or any similar words and expressions shall be construed as illustrative only and shall not limit the sense of any word, phrase, term, definition, or description preceding those words.

1.2.6. a reference to 'writing' or 'written' includes any method of reproducing words in a legible and non-transitory form (including email).

1.2.7. references to any applicable laws shall be references to any applicable laws replacing, amending, extending, re-enacting, or consolidating any such applicable laws and the equivalent terms defined in such applicable laws, once in force and applicable; and

1.2.8. a reference to any law includes all subordinate legislation made from time to time under that law.

2. SCOPE AND APPLICATION OF THIS AGREEMENT

2.1. This DPA applies to the processing of End User Data by the Service Provider on behalf of the Licensee pursuant to the Master Services Agreement.

2.2. This DPA shall continue in full force and effect for the term of the Master Services Agreement and will automatically and immediately terminate upon termination or expiry of the Master Services Agreement for any reason.

3. PROCESSING OF PERSONAL DATA & INSTRUCTIONS

3.1. The parties acknowledge and agree that with regard to the processing of End User Data, the Licensee shall be the Controller and the Service Provider is a processor (except where the Licensee is a processor to a third-party Controller, in which case the Service Provider shall be a sub-processor).

3.2. The Service Provider shall process End User Data solely for the purpose of providing the AHI Services to the Licensee and only in accordance with the Licensee's instructions (including processing initiated by End Users in their use of the Services) or as otherwise necessary to comply with applicable laws. Information about the means of processing, including hosting and technical architecture information, are provided at Schedule 3.

3.3. The Licensee's instructions shall only be constituted by:

3.3.1. the Master Services Agreement and this DPA.

3.3.2. the Licensee or any End User uploading or otherwise entering End User data into the AHI Platform.

3.3.3. any settings selected and/or configurations made or initiated by the Licensee or any End User in or to the AHI Platform or in respect of the AHI Services.

3.3.4. any reasonable written instructions provided by the Licensee to the Service Provider via email or through any communications tool facilitated by the AHI Services which are expressly stated to be written instructions issued by the Licensee as Controller to the Service Provider as processor and which are consistent with the terms of the Master Services Agreement and this DPA; or

3.3.5. the Licensee and relevant End-Users using the functionality of the AHI Platform or provided as part of the AHI Services to issue instructions to process Personal Data, such as, to delete Personal Data or export Personal Data.

3.4. The Licensee shall ensure that its instructions comply with Data Protection Law, and the Service Provider shall not be required to comply with the Licensee's instructions if such instructions would violate Data Protection Law or any other law or regulation.

3.5. The parties acknowledge and agree that with regard to the processing of Account Data and Service Data, the Service Provider is an independent Controller, and the Service Provider shall process Account Data and Service Data in accordance with Data Protection Law.

4. LICENSEE'S OBLIGATIONS

4.1. The Licensee shall, in its use of the AHI Platform and AHI Services, process End User Data in accordance with the requirements of Data Protection Law and shall have sole responsibility for the accuracy, quality and legality of End User Data and the means by which it has acquired End User Data; and represents and warrants to the Service Provider that:

4.1.1. it has complied and will continue to comply, with Data Protection Law in respect of its processing of End User Data.

4.1.2. it has provided, and will continue to provide, all necessary notices (including any applicable requirements to provide notice to End Users regarding the use of the Service Provider as a processor) and has obtained, and will continue to obtain, all Consents and rights necessary under Data Protection Law for the Service Provider to process End User Data for the purposes described in this DPA.

4.1.3. it has and will continue to have, the right to upload or transfer End User Data to the AHI Platform for processing in accordance with the terms of the Master Services Agreement and this DPA; and

4.1.4. The processing of End User Data by the Service Provider for the purposes of the Services will not violate the rights of any Data Subject that has opted out from sales.

4.2. The Licensee undertakes not to upload or transfer (or cause to be uploaded or transferred) any Sensitive Data (excluding any End User Data created by or using the AHI Service) or any Personal Data relating to any Data Subject who is not an End User to the AHI Platform, and agrees that the Service Provider shall have no liability whatsoever for any such Sensitive Data (with the exception of End User Data created by or using the AHI Service) or third party Personal Data, whether in connection with a Personal Data Breach or otherwise.

5. SUB-PROCESSING

5.1. The Service Provider shall be entitled to use sub-processors to process End User Data for the purpose of providing the AHI Services. For these purposes, the Licensee authorises the use of the sub-processors listed at Schedule 2.

5.2. If the Service Provider intends to use any new sub-processor to process End User Data for the purpose of providing the AHI Services, it shall notify the Licensee thereof in writing following which the Licensee shall have 30 days to object, on reasonable grounds, to the use of any such new sub-processor. If no objection is raised, the Licensee shall be deemed to have authorised the new sub-processor for the purposes of clause 5.1, above. If the Licensee raises an objection, the parties shall meet (in person, by telephone or by video call) within 7 days of such objection to discuss commercial reasonable alternative solutions in good faith. If the parties cannot reach a resolution in 30 days, the Service Provider shall be entitled to terminate the Master Services Agreement by written notice.

5.3. Before using any sub-processor to process End User Data, the Service Provider shall enter into a sub-processing contract with the sub-processor that meets the requirements of Data Protection Law.

5.4. In the event that a sub-processor used by the Service Provider to process End User Data for the purpose of providing the AHI Service fails to meet its obligations under a sub-processing contract with the Service Provider, the Service Provider shall remain fully liable to the Licensee for failing to meet its obligations under this DPA.

6. SECURITY & CONFIDENTIALITY

6.1. The Service Provider has implemented and will maintain the technical and organisational measures set out at Schedule 1 (the "Security Measures") to protect End User Data against unauthorised or unlawful processing, accidental loss, destruction, damage, alteration, or disclosure.

6.2. The Licensee acknowledges and agrees that:

6.2.1. the Security Measures provide a level of security for End User Data that is appropriate for the risk to End Users associated with the processing of End User Data, taking in to account the, the costs of implementation and the nature, scope, context, and purposes of processing; and

6.2.2. that the security measures are subject to technical and organisational progress, and development, threat landscape and risk posture and that the Service Provider may update or modify the Security Measures from time to time, provided that such updates do not result in the degradation of the overall security of the AHI Service or protection of End User Data.

6.3. The Service Provider shall ensure that any person who is authorised by it to process End User Data (including its staff, agents, and subcontractors) shall be under a contractual obligation of confidentiality.

7. REPORTING & NOTIFICATION of PERSONAL DATA BREACHES

7.1. The Service Provider shall notify the Licensee about any Personal Data Breach without undue delay and in any event within 48 hours (48) hours of identifying the Personal Data Breach.

7.2. The Licensee acknowledges and agrees that the Service Provider is subject to the *Australian Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) ("NDB Law"), meaning it will be deemed to 'jointly hold' the End User Data with the Licensee for the purposes of the NDB Law and will be required, following a Personal Data Breach to assess whether a reasonable person would conclude that the Personal Data Breach is likely to result in serious harm to affected individuals and if so, to notify the affected Data Subjects and the Office of the Australian Information Commissioner.

7.3. The Licensee acknowledges and agrees that if it is subject to the provisions of the UK GDPR or the EU GDPR, it will need to notify the appropriate Supervisory Authority of a Personal Data Breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of Data Subjects.

7.4. The Licensee acknowledges and agrees that if it is subject to the provisions of the UK GDPR or the EU GDPR, it will need to notify the Data Subjects affected by a Personal Data Breach

without undue delay, if the Personal Data Breach is likely to result in a high risk to their rights and freedoms.

8. RECORDS, AUDIT & ASSISTANCE

8.1. Where required by Data Protection Law, the Service Provider shall:

8.1.1. make available to the Licensee such information that is in its possession or control as is necessary to demonstrate the Service Provider's compliance with Data Protection Law; and

8.1.2. allow for and contribute to audits, including inspections, by the Licensee (at the Licensee's cost) to enable to Licensee to assess and verify the Service Provider's compliance with Data Protection Law (subject to a maximum of no more than one audit request in any 12-month period).

8.2. Where required by Data Protection Law, the Service Provider shall (at the Licensee's cost), assist the Licensee in complying with its obligations under Data Protection Law including to a defined Scope of Work by:

8.2.1. notifying the Licensee without undue delay if it receives a request from an End User to exercise their rights under Data Protection Law or any other compliant or request relating to the processing of the End User data.

8.2.2. cooperating fully with the Licensee and assisting as required in relation to any such End User request, compliant or other request by providing such End User Data and information as the Licensee reasonably requires; and

8.2.3. providing reasonable assistance to the Licensee in complying with its obligations under Data Protection Laws with respect to the security of processing, notification of Personal Data breaches, carrying out data protection impact assessments and in its dealings with data protection supervisory authorities.

8.3. Any costs payable by the Licensee under this clause 8 shall be charged by the Service Provider at its standard hourly rates and shall be payable by the Licensee within 7 days of invoice, except where charging for any of the access, information or assistance covered in this section is prohibited by Data Protection Law.

9. INTERNATIONAL TRANSFERS

9.1. The Licensee acknowledges and agrees that in connection with the provision of the AHI Services, End User Data will only be transferred to or accessible by AHI personnel based in Australia or sub-processer NuraLogix, documented in Schedule 2 – Sub Processors in Canada, for the provision of support services; and unless otherwise agreed in writing, will be hosted in the most relevant region, or as specifically requested by the Licensee.

9.2. The Service Provider may transfer 'personal information' for the purposes of the Australian Privacy Act 1988 (Cth) to the relevant region provided that it complies with Australian Privacy Principle 8 (Cross-border disclosure of personal information).

9.3. The Service Provider will also adhere to any other applicable Data Protection Law when transferring Personal Data internationally.

10. DELETION & DEIDENTIFICATION OF DATA

10.1. Subject as set out at clause 10.2, the Service Provider shall, at the request of the Licensee, delete all End User Data (unless retention of End User Data is required by law, in which case the Service Provider shall inform the Licensee of such requirement in writing) or return it to the Licensee (in the format reasonably requested by the Licensee) within a reasonable time after the earlier of the following:

10.1.1. termination of the Master Services Agreement; or

10.1.2. where processing of that End User Data is no longer required for the performance of the Service Provider's obligations under this DPA or the Master Services Agreement.

10.2. Before deleting or returning End User Data to the Licensee in accordance with clause 10.1, the Service Provider shall be permitted to anonymise and aggregate End User Data such that it fully ceases to include Personal Data ("Deidentified Data") and to keep and use the Deidentified Data for the purposes of improving and developing the AHI Services following termination of the Master Services Agreement and this DPA.

11. GENERAL

11.1. Amendment: This DPA represents the entire agreement between the parties with respect to its subject matter and may not be amended except by a written document executed by the parties. Notwithstanding the foregoing provisions of this paragraph, the Service Provider may amend this DPA by written notice to the Licensee ("Amendment Notice") if and to the extent the amendment is necessary to comply with Data Protection Laws or any amendments made to them, or the requirements of any applicable supervisory, government or regulatory authority. If the Licensee does not agree with any Amendment Notice, it must notify the Service Provider by written notice of that fact within 7 days of the date of the Amendment Notice ("Objection Notice"). If the parties are unable to resolve the objection within 7 days from the date of the Objection Notice ("Dispute Resolution Period"), either party may terminate this DPA for its convenience by written notice within 7 days of the expiry of the Dispute Resolution Period.

11.2. Assignment: Neither party may assign, transfer, licence or novate its rights or obligations under this DPA without the prior written Consent of the other party.

11.3. Severability: If any provision of this DPA is deemed invalid by a court of competent jurisdiction, the remainder of this DPA shall remain enforceable. If a provision of this DPA

conflicts with any Data Protection Law affecting the parties' commercial relationship, that provision will be severed and the remainder of this will remain enforceable.

11.4. Relationship: The parties are independent contractors and this DPA does not create any relationship of partnership, joint venture, or employer and employee or otherwise.

11.5. Counterparts: This DPA may be executed in counterparts provided that no binding agreement shall be reached until the executed counterparts are exchanged.

11.6. Entire Agreement: This DPA and any terms implied herein by any applicable Data Protection Laws constitute the entire agreement between the parties and to the extent possible by law, supersedes all prior understandings, representations, arrangements, and agreements between the parties, regarding its subject matter.

11.7. Applicable Law: This DPA will be governed by and construed in accordance with the law of the Master Services Agreement. To the extent this Data Processing Agreement is inconsistent with any other provision of the Master Services Agreement, this Master Services Agreement shall prevail.

SCHEDULE 1: SECURITY MEASURES

The Service Provider has implemented the following technical and organisational security measures:

- Information security policies and related procedures
- Staff security awareness straining
- Security and data protection obligation in AHI's Policies and Procedures for employees, and subcontractors
- Identity and access management measures including identity verification, multi-factor authentication and authorisation processes in respect of all computer systems
- Anti-malware software, email web filtering and security detection and protection software.
- Physical security measures at all buildings and offices, include door and window locks, filing cabinet locks and visitor access management controls.
- Network boundary protection controls, including firewalls
- Security testing including penetration testing of software developed by the Service Provider (including the AHI software development kit or 'SDK').
- Data backup and archiving supporting by business continuity and IT disaster recovery plans.
- Where necessary, taking in to account the state of the art, the costs of implementation and the nature, scope, content, and purpose of the processing, pseudonymisation and/or encryption of Personal Data.

<< The remainder of this page is intentionally left blank >>

SCHEDULE 2: SUB-PROCESSORS

The following sub-processors are authorised by the Licensee to End-User Data:

Sub-Processor	Purpose	Location
NuraLogix Corporation (“NuraLogix”)	Face Scan processing Services	Canada
Amazon Web Services	Public Cloud Services	Global
Itoc Pty Ltd	24x7 Monitoring of the AHI Platform	Australia

<< The remainder of this page is intentionally left blank >>

SCHEDULE 3: NATURE, MEANS & PURPOSES OF PROCESSING

Part A: Overview

The Service Provider Processes End User Data on behalf of the Licensee for the purpose of providing smartphone and cloud based digital biometric processing services.

The Service Provider processes:

- Face Scan Data to calculate heart rate, irregular heartbeats, breathing, blood pressure, heart rate variability, and cardiac workload information, as well as provide support to End Users.
- Body Scan Data to calculate digital anthropometric circumference measurements, body composition information (such as body fat %), and to provide support to End Users.

The AHI Platform is hosted on the cloud platforms managed by leading cloud service provider.

AHI regularly test our SDK for vulnerability to Open Web Application Security Project standards by independent security experts.

BodyScan

All BodyScan data processing happens on-device. No End-User images or videos ever leave their device, as all measurements are processed on-device.

To process and return Body Scan results, no Personally Identifiable Information leaves the End-User's device.

FaceScan

FaceScan data is processed on AWS cloud. AHI's cloud service provider locations are global; however, the processing of the End-User's data is based on the geographic proximity of the End-User's public IP address.

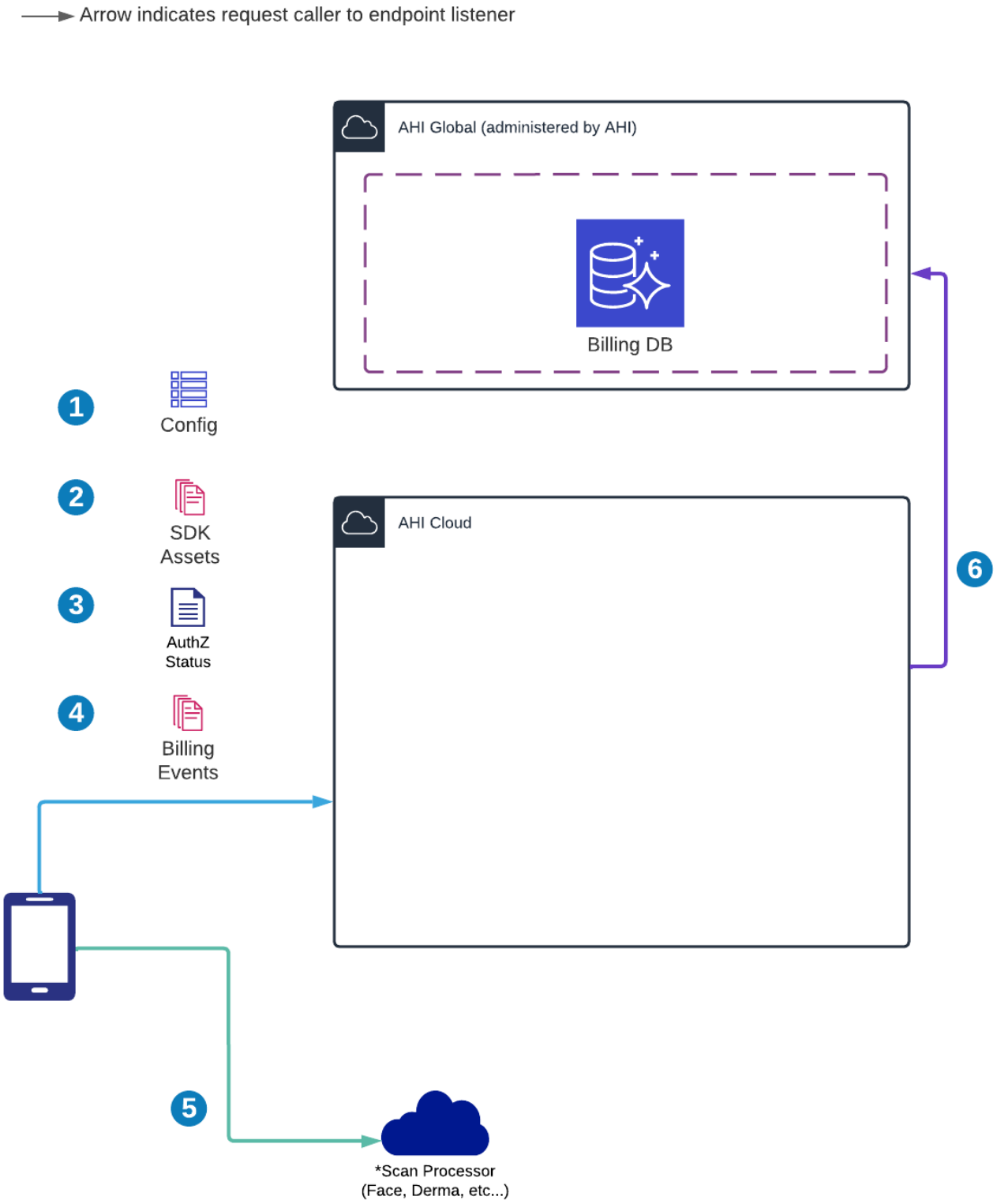
When the End-User requests a FaceScan, if they are located in the EU for example, the request will be processed in the EU cloud service provider's regional location.

The signals (facial blood flow data) are extracted from the FaceScan video and encrypted at rest and on transmission.

All Personally Identifiable Information is deleted after processing.

The diagram at Part B (image below) shows the AHI Platform architecture as of the commencement date of this DPA.

Part B: Architecture



Description:

1. Client specific configuration details when setup() is called.
2. SDK remote resources to be downloaded.
3. User authorization.
4. Billing events.
5. FaceScan processing service (only signal data sent, not personally identifiable user data).
6. Billing data is passed through to AHI Global billing Database.