INCODE END-USER AGREEMENT

This End User Agreement (Federal) (Channel Partner) **("Agreement")** shall govern the rights and obligation of the Federal Government agency end user licensee ("Customer") to use the Products (as defined in Section 13 (Definitions)) of Incode Technologies Inc. ("Incode") when purchased through a prime contractor Carahsoft Technology Corp. ("Carahsoft" or "Company").

1. **License Grant.** During the term of ______________months ("Term"), Incode hereby grants Customer a nonexclusive, limited, personal, nonsublicensable, nontransferable right and license to use and access the Products only for the internal business purposes of Customer, and only in accordance with Incode's Documentation (as defined in Section 12 (Definitions)). No other rights or licenses are granted except as expressly and unambiguously set forth herein.

2. **License Restrictions.** Customer shall not (and shall not permit any third party to), directly or indirectly: (a) reverse engineer, decompile, disassemble, or otherwise attempt to discover the underlying structure of the Product (except to the extent applicable laws specifically prohibit such restriction); (b) modify, translate, or create derivative works based on the Product; (c) transfer or encumber rights to the Product; (c) use the Product for the benefit of a third party; (d) remove or otherwise alter any proprietary notices from the Product or any portion thereof; (e) use the Product to build an application or product that is competitive with any Incode product or service; (f) interfere or attempt to interfere with the proper working of the Product or any activities conducted on the Product; (g) bypass any measures Incode may use to prevent or restrict access to the Product (or other accounts, computer systems or networks connected to the Product); (h) use the Product for the design or development of nuclear, chemical or biological weapons or missile technology, or for terrorist activity, without the prior permission of the United States government; or (i) allow any third party to remove or export from the United States or Mexico or allow the export or re-export of any part of the Software or any direct product thereof (i) into (or to a national or resident of) any embargoed or terrorist-supporting country, (ii) to anyone on the U.S. Commerce Department's Table of Denial Orders or U.S. Treasury Department's list of Specially Designated Nationals, (iii) to any country to which such export or re-export is restricted or prohibited, or as to which the United States government or any agency thereof requires an export license or other governmental approval at the time of export or re-export without first obtaining such license or approval or (iv) otherwise in violation of any export or import restrictions, laws or regulations of any United States or foreign agency or authority. Customer is responsible for all of Customer's activity in connection with the Product, including but not limited to uploading Customer Data onto the Product. Customer warrants that it is not located in, under the control of or a national or resident of any such prohibited country or on any such prohibited party list. Customer (A) shall use the Product in compliance with all applicable laws, treaties and regulations in connection with Customer's use of the Product, and (B) shall not use the Product in a manner that violates any third party rights. **This provision shall survive any expiration or termination of this Agreement.**

3. **Customer Data.** Incode will be provided and process certain of Customers' data **("Customer Data")** to perform its obligations under this Agreement. Customer is solely responsible for the accuracy, integrity, and legality of Customer Data. Customer represents and warrants that it owns all right, title and interest in and to the Customer Data or otherwise has sufficient rights to the Customer Data to permit its use as contemplated hereunder. Incode is not responsible to Customer for unauthorized access to Customer Data or the unauthorized use of the Product. The parties acknowledge and agree that any data personal and specific to an individual is owned by such individual. Customer acknowledges and agrees that Incode may (a) internally use and modify (but not disclose) Customer Data for the purposes of (i) improving the Product and providing the Product to Customer and (ii) generating Aggregated Anonymous Data (as defined below); and (b) freely use and make available Aggregated Anonymous Data for Incode's business purposes (including without limitation, for purposes of improving, testing, operating, promoting and marketing Incode's products and services) notwithstanding anything herein to the contrary. "Aggregated Anonymous Data" means data submitted to, collected by, or generated by Incode in connection with Customer's use of the Product in aggregated, anonymized form which cannot be linked to Customer or identifies any User. **This provision shall survive any expiration or termination of this Agreement.**

4. **Consent in respect of End Users**. Before any Customer end user ("End-User") accesses the Products and prior to the collection of their selfie and government issued identification document: **(i)** Customer agrees to display the joint consent language included in part I of Exhibit 1 ("Joint Consent Language") on its website and/or application to End-Users located in the United States. Customer must provide Incode with such consent agreement by the End-User in real-time for Incode's record keeping purposes. In case any End-User does not provide consent to Customer verifying their identity through the Products (by ticking the first checkbox of the Joint Consent Language), Customer shall not allow such End-User to access the Products and doing otherwise shall be a material breach of this Agreement by Customer. In relation to the provision of Products in the United States, Customer acknowledges and agrees that if Customer only purchases onboarding services from Incode, Biometric Information (as defined in Exhibit 1), shall be deleted by Incode immediately upon the cessation of the provision of Products to

End-Users to comply with applicable laws and that therefore, in the event that Customer decides to purchase authentication services from Incode in the future, additional consent to process Biometric Information shall be requested by the Customer. **(ii)** Simultaneously with Customer, Incode shall be entitled to process the End-User's personal data, including Biometric Data (i.e. "End-User Data") once it has requested the End-Users' consent, to improve its products and services, including the Products, through the second checkbox of the Joint Consent Language; for the avoidance of doubt, Incode shall only process End-User Data in the event the End-User has provided their consent to Incode. Notwithstanding the foregoing, Incode may retain End-User Data, including Biometric Data, for such longer period as permitted under applicable laws.

5. **Consent in respect of other End Users**. Before any End-User accesses the Products and prior to the collection of their selfie and government issued identification document: **(i)** If Customer is required to request consent from its End-Users to be able to process their personal data to provide the Products, Customer shall not allow the End-User to access the Products if such consent is not obtained and doing otherwise shall be a material breach of this Agreement by Customer, however if Customer has a legitimate basis to process the Customer Data as stated above, then only the following section (ii) shall apply; **(ii)** Incode shall be entitled to display, the consent wording set forth in Exhibit D for the purpose of improving its products and services, including the Products, in accordance with the above provisions, for the avoidance of doubt, Incode shall only process personal data, including Biometric Data, for such purposes so long as the end-user has provided its consent to Incode.

6. **Updates to Exhibit 1**. If the consent wording in Exhibit 1 needs to be amended for a specific territory, the parties will work together in implementing such adjustments, in the understanding that the Products will not be provided by Incode until required adjustments are made to comply with applicable laws in such territories.

Where Customer is required to obtain consent from end-users in order to provide the Products under applicable laws and in accordance with the above provisions, Customer shall be responsible for implementing a consent request and to provide Incode with the end-users' consent agreements in real-time in order for Incode's own record keeping purposes. Incode shall implement its own consent request as set out above.

7. **Third Party Services.** Customer acknowledges and agrees that the Products may use services provided by third parties ("Third Party Services"). Incode is not responsible for the operation of any Third Party Services nor the availability or operation of the Products to the extent such availability and operation is dependent upon Third Party Services. Customer is solely responsible for procuring any and all rights necessary for it to access Third Party Services and for complying with any applicable terms or conditions thereof. Incode does not make any representations or warranties with respect to Third Party Services or any third party providers. Any exchange of data or other interaction between Customer and a third party provider is solely between Customer and such third party provider and is governed by such third party's terms and conditions. The Software may incorporate third-party open source software ("OSS"). To the extent required by the OSS license, that license will apply to the OSS on a stand-alone basis.

8. **Suspension; Effect of Termination.** Incode may temporarily suspend or limit Customer's access to or use of the Products if Customer's use of the Products results in (or is reasonably likely to result in) damage to or material degradation of the Products which interferes with Incode's ability to provide access to the Products to other Incode customers. Such suspension or limitation shall be only as long as necessary to mitigate the concerns leading to such suspension or limitation. Upon expiration or earlier termination of this Agreement, all license granted to Customer will cease, and Customer must immediately cease using the Products and delete (or, upon request, return) all copies of the Products, including, without limitation, any and all Software. At Incode's request, Customer will delete all of Incode's Confidential Information. Confidential Information may be retained in Incode's standard backups after deletion but will remain subject to the Agreement's confidentiality and non-use restrictions. In no event will Incode refund any amounts paid for use of the Products. **This provision shall survive any expiration or termination of this Agreement.**

9. **Disclaimer of Warranties.** INCODE WARRANTS THAT THE PRODUCTS WILL, FOR A PERIOD OF SIXTY(60) DAYS FROM THE DATE OF YOUR RECEIPT, PERFORM SUBSTANTIALLY IN ACCORDANCE WITH THE PRODUCTS WRITTEN MATERIALS ACCOMPANYING IT. EXCEPT AS EXPRESSLY SET FORTH IN THE FOREGOING, THE PRODUCTS ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND ARE WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES IMPLIED BY ANY COURSE OF PERFORMANCE, USAGE OF TRADE, OR COURSE OF DEALING, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. INCODE DOES NOT WARRANT THAT CUSTOMER'S USE OF THE PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE OR THAT ANY SECURITY MECHANISMS IMPLEMENTED BY THE PRODUCTS WILL NOT HAVE INHERENT LIMITATIONS. **This provision shall survive any expiration or termination of this Agreement.**

10. Limitation of Liability. EXCEPT FOR CUSTOMER'S BREACH OF THE LICENSE RESTRICTIONS OF THE AGREEMENT OR EITHER PARTY'S BREACH OF ITS CONFIDENTIAITY OBIGATIONS, IN NO EVENT SHALL EITHER PARTY, NOR ITS DIRECTORS, EMPLOYEES, AGENTS, PARTNERS, SUPPLIERS OR CONTENT PROVIDERS, BE LIABLE UNDER CONTRACT, TORT, STRICT LIABILITY, NEGLIGENCE OR ANY OTHER LEGAL OR EQUITABLE THEORY WITH RESPECT TO THE SUBJECT MATTER OF THE AGREEMENT (A) FOR ANY LOST PROFITS, DATA LOSS, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES OF ANY KIND WHATSOEVER, SUBSTITUTE GOODS OR SERVICES (HOWEVER ARISING), (B) FOR ANY BUGS, VIRUSES, TROJAN HORSES, OR THE LIKE (REGARDLESS OF THE SOURCE OF ORIGINATION), OR (C) FOR ANY DIRECT DAMAGES IN EXCESS OF (IN THE AGGREGATE) THE FEES PAID (OR PAYABLE) TO INCODE FOR THE PRODUCTS/SERVICES WITH RESPECTO TO THE LICENSE GRANTED HEREUNDER IN THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO A CLAIM HEREUNDER. TO THE EXTENT THE FOREGOING IS LIMITED BY THE ANTI-DEFICIENCY ACT OR OTHER APPLICABLE LAWS, THE LIMITATION OF LIABILTY FOR BOTH PARTIES WILL BE SUBJECT TO THE LIMITS IMPOSED ON CUSTOMER BY THE ANTI-DEFICIENCY ACT OR SUCH OTHER APPLICABLE LAWS. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) FRAUD; (2) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW. **This provision shall survive any expiration or termination of this Agreement.**

11. Government End Users. The Products are "commercial products" (as defined at Federal Acquisition Regulation (FAR) 2.101) and are "commercial computer software" (as defined at FAR 2.101). If the Customer of the Products is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Products, Software or any related Documentation of any kind, including technical data and manuals, is restricted by the terms of this Agreement in accordance with FAR 12.212 for civilian agency use and Defense Federal Acquisition Regulation Supplement (DFARS) 227.7202 for military purposes. All other use is prohibited. If any Federal Customer has a need for rights not conveyed under the terms described in this Section, it must negotiate with Incode to determine if there are acceptable terms for transferring such rights, and a mutually acceptable written and signed addendum specifically conveying such rights must be included in any applicable contract or agreement to be effective. If this Agreement fails to meet the Government's needs or is inconsistent in any way with Federal law, and the parties cannot reach a mutual agreement on terms for this Agreement, the Government agrees to terminate its use of the Products and Documentation and stop any use of, and return or destroy, the Products (including Software and Documentation) and any other software or technical data delivered as part of the Products and Documentation to Incode. This Government End Users clause in this Section is in lieu of, and supersedes, any other FAR, DFARS, or other clause, provision, or supplemental regulation that addresses Government rights in computer software or technical data under this Agreement. **This provision shall survive any expiration or termination of this Agreement.**

12. Definitions (This provision shall survive any expiration or termination of this Agreement):

- "**Confidential Information**" means information disclosed under this Agreement that is designated by the disclosing party as proprietary or confidential or that should be reasonably understood to be proprietary or confidential due to its nature and the circumstances of its disclosure. Incode's Confidential Information includes the Software and any technical or performance information about the Software.
- **"Documentation"** means Incode's usage guidelines and standard technical documentation for the Software. For purposes of this Agreement, Documentation means Incode's usage guidelines and standard technical documentation for the Software, the current version of which is available at:
  - 1. SDK Web: https://docs.incodesmile.com/
  - 2. API Rest: https://incodeomni.docs.apiary.io
  - 3. Native SDK Android: https://github.com/IncodeTechnologies/Incode-Welcome-Android-example
  - 4. Native SDK iOS: https://github.com/IncodeTechnologies/Incode-Welcome-Example-iOS
- **"End User"** or **"End-User"** means the ultimate individual accessing the Service.
- **"Product"** or **"Products"** means any equipment, licensed Software, and/or support/maintenance subscriptions which the parties are authorized to procure, for resale or distribution sales only, under this Agreement, including SAAS (as defined herein below).
- **"SAAS"** means (a) access to the Software, and (b) any other services provided by Incode
- "**Software**" means Incode's generally available off-the-shelf proprietary software technology product and related APIs. The Software includes the Documentation and any updates but does not include Third Party Services (as defined herein).

13. Indemnification. Incode will have the right to intervene to defend Customer from and against any third-party claim to the extent alleging that the Software, when used by Customer as authorized in this Agreement, violates a third party's United States patent, copyright, trademark or trade secret, and will indemnify and hold harmless Customer against any damages or costs awarded against Customer (including reasonable attorneys' fees) or agreed in settlement by Incode resulting from the claim. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

In response to an actual or potential infringement claim, if required by settlement or injunction or as Incode determines necessary to avoid material liability, Incode may at its option: (a) procure rights for Customer's continued use of the Software, (b) replace or modify the allegedly infringing portion of the Software to avoid infringement without reducing the Software's overall functionality or (c) terminate the affected Order and refund to Customer any pre-paid, unused fees for the terminated portion of the Subscription Term. Incode's obligations in this Section 13 do not apply to: (i) infringement resulting from Customer's modification of the Software, (ii) any Third Party Services contained within the Software , (iii) the combination, operation or use of the Services with software and/or hardware not delivered by Incode if such infringement could have been avoided by combination, operation or use of the Service with other software and/or hardware, (iv) unauthorized use of the Software, (v) Customer's failure to follow the procedures set forth in herein below, or (v) to Software Evaluations or other free or evaluation use. Customer shall be solely liable for any claims by Customer's authorized end users arising from use of Third-Party Services and/or Customer's own Services or services. **This Section 13 sets out Customer's exclusive remedy and Incode's entire liability regarding infringement of third-party intellectual property rights.**

The indemnifying party's obligations in this Section 13 are subject to the indemnified party providing (a) prompt notice of any claim, (b) the exclusive right to defend and settle such claim and (c) at the indemnifying party's request and expense, all reasonably necessary cooperation of the indemnified party with such defense and settlement efforts. The indemnifying party may not settle or make any admissions about any claim without the indemnified party's prior consent if settlement would require the indemnified party to admit fault or take or refrain from taking any action (other than relating to use of the Software, when Incode is the indemnifying party). Subject to the foregoing, the indemnified party may participate in a claim with its own counsel at its own expense.

This provision shall survive any expiration or termination of this Agreement.

14. Confidentiality. As the receiving party, each party will (a) hold in confidence and not disclose Confidential Information to third parties except as permitted in this Agreement and (b) only use Confidential Information to fulfill its obligations and exercise its rights in this Agreement. The receiving party may disclose Confidential Information to its employees, agents, contractors and other representatives having a legitimate need to know, provided the receiving party remains responsible for the compliance of such representatives with this Section 14 and such representatives of the receiving party are bound to confidentiality obligations no less protective than this Section 14. These confidentiality obligations do not apply to information that the receiving party can document (i) is or becomes public knowledge through no fault of the receiving party, (ii) it rightfully knew or possessed prior to receipt under this Agreement, (iii) it rightfully received from a third party without breach of confidentiality obligations or (iv) it independently developed without using the disclosing party's Confidential Information. The receiving party may disclose Confidential Information if required by law, subpoena or court order, provided (if permitted by law) the receiving party notifies the disclosing party in advance and cooperates in any effort to obtain confidential treatment. Incode recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor. The parties acknowledge that unauthorized use or disclosure of Confidential Information may cause substantial harm for which damages alone are an insufficient remedy. Each party may seek appropriate equitable relief, in addition to other available remedies, for breach or threatened breach of this Section 14.

This provision shall survive any expiration or termination of this Agreement.

15. Miscellaneous

- Applicable Law. This Agreement is governed by the Federal laws of the United States without regard to its conflicts of laws provisions and without regard to the United Nations Convention on the International Sale of Goods. Any dispute or claim arising out of or in connection with this Agreement or the performance, breach or termination thereof, shall be finally settled by the federal Courts in the State of California.

- Waivers and Severability. Waivers must be signed by the waiving party's authorized representative and cannot be implied from conduct. If any provision of this Agreement is held invalid, illegal or unenforceable, it will be limited to the minimum extent necessary, so the rest of this Agreement remains in effect.

- Notices. Notices and consents under this Agreement must be in writing to the following address(es):

Customer. ______________________	Incode. 101 Mission Street, Suite 900, San Francisco CA 94105 / LegalCompliance@incode.com

  Either party may update its address with notice to the other party. Incode may also send operational notices to the Customer by email to the contact information specified herein.

- Force Majeure. In accordance with GSAR Clause 552.212-4(f), Neither party is liable for any delay or failure to perform any obligation under this Agreement (except for a failure to pay fees) due to events beyond its reasonable control, such as a strike, blockade, war, act of terrorism, riot, Internet or utility failures or infrastructure services provided by third parties, epidemic, pandemic, refusal of government license or natural disaster.
- Independent Contractors. The parties are independent contractors, not agents, partners or joint venturers.
- Entire Agreement & Counterparts. This Agreement is the parties' entire agreement regarding its subject matter and supersedes any prior or contemporaneous agreements regarding its subject matter. In this Agreement, headings are for convenience only and "including" and similar terms are to be construed without limitation. This Agreement may be executed in counterparts (including electronic copies and PDFs), each of which is deemed an original and which together form one and the same agreement.

EXHIBIT 1
INCODE'S CONSENT REQUEST

Customer agrees to include the following consent modules before End-Users may access the Products, through an un-checked checkbox module:

[COMPANY LEGAL NAME] ("Company") uses technology from Incode Technologies, Inc. ("Incode") for identity verification, fraud prevention, and security purposes ("Services"). Company and/or Incode may collect biometric identifiers and biometric information, such as your faceprint ("Biometric Data"), a selfie image, and, where applicable, information from your government-issued identification [or your interactions with Incode and Company systems while onboarding (collectively with Biometric Data, "Personal Data") for the Services, and may disclose such data to service providers or government entities that facilitate the Services, or as required by law.

LEARN MORE *about how your Personal Data is processed, stored, and protected at: [COMPANY AND INCODE ATTACHED POLICIES and TERMS OF USE]*

Consent for Biometric Processing:
By ticking this box I consent to the capture, collection, enrollment, use, retention, processing, and disclosure of a scan of my face geometry (i.e. faceprint) and information derived from the barcode of the identification card I provide as follows:

- *Purpose: verifying my identity pursuant to Incode's Privacy Policy*
- *Data Collected: facial geometry/faceprint/image; data contained in/obtained by scanning the barcode of a government-issued identification card provided by me (including, e.g., name, address, DOB, license type, sex, height, weight, eye color, ID number)*

- *Retention Period: earliest of: (i) so long as necessary for identity verification purposes; or (ii) stated Data Retention Period (e.g. IL (3 yrs following last engagement), TX (1 yr following exhaustion of purpose)).*

□ *I have read and agree to the Privacy Policies of and Terms of Use of Company and Incode.*

Consent:

□ *By ticking this box I consent to the provision to Incode of my identification Personal Data, including my Biometric Data, for the purpose of improving, modifying, or updating Incode's products or services (including its algorithm) in accordance with the Incode Privacy Policy. I can exercise my privacy rights, including withdrawal of my consent, by contacting dataprotection@incode.com.*

IMPORTANT: *My consent is voluntary and will not affect Company's services.*

Attachment B

SUPPORT TERMS

This attachment sets forth the relationship between Incode and Company regarding the resolution of problems with the Incode Services and/or Software. Incode may update the terms and conditions below from time to time upon prior notice to Company and the new terms will be applicable to support and maintenance services thereafter. Capitalized terms that are not defined herein shall have the meaning set forth in the Aggregated Agreement by and between Incode and Company.

1. **CONTACTS**.

1.1 **Company Contact(s).** Company will designate the contact information of one (1) individual to act as support liaisons to utilize the support (the "**Company Contact(s)**") and will ensure that such person(s) will be properly trained in the operation and usage of the Software. All support services and communications shall be conducted solely through the Company Contact.

1.2 **Incode.** Incode will provide Company with technical support through the Company Contact(s) via the following methods: e-mail. Company may contact Incode via telephone during the hours of 8 a.m. to 5 p.m. Pacific Standard Time.

2. **SUPPORT OBLIGATIONS**.

2.1 **Incode Support.** Subject to Company's timely payment of the Support Fee, Incode shall provide Tier 3 support as set forth herein. Company shall be solely responsible for providing direct, and all other support, to Customers, for the Incode Services. Incode's software support obligation is limited to the production release of the Software authorized for use by the Company and Company´s Customers. Incode will not be obligated to provide support or maintenance services to any other individuals.

2.2 **Company Obligations.** Company agrees to provide reasonable access to all necessary personnel to answer questions about any problems reported by Company regarding the Services and/or Software. Company also agrees to promptly implement all updates and error corrections provided by Incode. Upon request, Company will provide access for on-line diagnostics of the Services and/or Software during error diagnosis. Incode will have no obligation to communicate with Customers, or any end users, unless specifically agreed to by Incode. Upon identification of any programming error, Company shall notify Incode of such error and shall provide Incode with enough information to reproduce the error. Incode shall not be responsible for correcting any errors not attributable to Incode. Incode shall only be responsible for errors that are reproducible by Incode on unmodified Software as delivered to Company.

2.3 **Error Corrections.** Incode shall use its reasonable efforts to correct any reproducible programming error in the Services and/or Software attributable to Incode with a level of effort commensurate with the severity of the error, provided that Incode shall have no obligation to correct all errors in the Software. Requests for error corrections to Incode can occur in two forms:

2.3.1 ***Request for a Bug Fix.*** Request a fix to resolve a problem for which there is a reproducible test case that demonstrates the problem.

2.3.2 ***Request for Technical Assistance.*** Request for assistance in diagnosing problems that do not have reproducible test cases, are usability related issues (such as performance tuning or configuration), are intermittent in nature, or require diagnosis against a configuration that is unavailable to Company.

2.4 **Special Services.** Company may request maintenance and support services not specifically provided for in this Agreement, which Incode may provide in its sole discretion. Company acknowledges that, if provided, all such services shall be at Incode's then-current term and conditions for such services.

2.5 **Software Modifications.** Incode may replace or repair the Software with either new or reconditioned software. Incode reserves the right to change or discontinue any Software at any time, subject to thirty (30) days' notice.

2.6 **Exclusions.** Support does not include services requested as a result of, or with respect to, causes which are not attributable to Incode or Incode Software ("**Excluded Services**"). Excluded Services will be billed to Company at Incode's then-current rates. Causes which are not attributable to Incode or Incode Software include, but are not limited to:

2.6.1 Errors that result from or are exacerbated by Company or Customer's, failure (i) to provide Incode access to the Incode Software to diagnose or fix errors;

2.6.2 installation, modification, customization, alteration or addition (or any attempt of the foregoing) of the Software undertaken by any party other than Incode or an authorized designee of Incode;

2.6.3 Errors arising out of misuse, abuse, misapplication, negligent or willful acts of Company, Customer, or any third party;

2.6.4 any unauthorized combination of Incode Software with third-party software not provided by Incode;
2.6.5 use of Incode Software other than in accordance with its documentation or the applicable End-User Attachment;
2.6.6 use of a version of Incode Software other than the specified production release;
2.6.7 failure to provide the minimum technical environment, as specified in applicable documentation.

3. **<u>TIERED SUPPORT DESCRIPTION</u>.** The following chart describes Tier 3 support.

Tier	**Description; Guidelines**
Tier 3	• Validation of product defect • Action plan definition • Fix software bugs or generate work-arounds • Troubleshoot bugs, cases and issues • Escalate case to engineering for bug fix • Coordinate software patches with Company support and organization. For clarity, support will include: (a) assistance related to questions on the installation and operational use of the Software; (b) assistance in identifying and verifying the causes of suspected errors in the Software; and (c) providing workarounds for identified Software errors or malfunctions, where reasonably available to Incode.

Privacy Policy

Last Modified: February 22, 2024

Welcome to Incode Technologies, Inc. (“Incode,” “we,” “our” and “us”). Please read this Privacy Notice to learn about who we are, how we collect, disclose and use your personal data and how you can exercise your privacy rights.

You may print a copy of this Privacy Notice directly from your browser. If you have a disability, you may access this Privacy Notice in an alternative format by contacting us at dataprotection@incode.com.

If you have any questions or concerns about our use of your personal data, then please contact us using the contact details provided at the bottom of this Privacy Notice.

Quick Links

1. What does Incode do?

Incode is headquartered in the United States and has offices and group companies located around the world. Incode provides Incode Omni, an end-to-end identity platform that offers a frictionless customer experience at every point of contact across multiple channels. Incode Omni is deployed on third-party websites or mobile applications that belong to our customers ("Customers") and allows our Customers to securely verify the identity of their customers or users ("Users"). You can find more information about us and Incode Omni here. Incode also offers IncodeID, a direct-to-consumer, frictionless identity verification platform that allows IncodeID users to verify their identity with companies that accept IncodeID.

2. What does this Privacy Notice cover?

This Privacy Notice covers our collection, use and disclosure of personal data that we gather in the usual course of business, for example, through our website at incode.com, including its subdomains such as docs.incode.com (the "Website"), when you access or use IncodeID or Incode Omni (the "Products"), through responses to surveys or questionnaires, when you send us an email or otherwise contact us or at offline locations and events (all together, the "Services"). In such case, we act as a data controller of your personal data.

Please note that we also act as a processor when providing identity verification services to certain of our Customers. This Privacy Notice does not apply to the personal data that we process as a data processor on behalf of our Customers in the course of providing Incode Omni. In those cases, we invite you to contact the relevant company or organization if you have any questions about their privacy practices.

We may provide you with additional privacy notices depending on how you interact with us and depending on the type of personal data we collect.

3. Sources of personal data

We may obtain your personal data from the following sources:

- **Directly from you**, such as when you use or access the Services, communicate or transact through the Website, or submit personal data online in connection with the Services.
- **Our vendors**, such as when our vendors provide us personal data related to you in the process of providing us their services.
- **Cookies and other similar technologies**, such as when you visit the Website, which may have first- and third-party tools (e.g., cookies) that help facilitate and personalize your visit to the Website or to other online services. For more information, see the section titled “Cookies and other similar technologies.”
- **External sources**, such as from publicly available government records and our business partners, in connection with co-marketing or other joint marketing campaigns. This does not include our vendors.

4. What personal data does Incode collect and why does Incode collect it?

The personal data we collect depends on the context of your interactions with Incode and the choices you make (including your privacy settings), the products and features you use, your location and applicable law. The chart below details our current practices and our practices for the 12 months preceding the Last Modified date. Note that the specific pieces of personal data we have collected about you may vary depending on the nature of your interactions with us and may not include all of the examples below.

Category of personal data	Purposes for collection, use and disclosure
Identifiers, such as a real name, postal address, unique personal identifier (e.g., logins and passwords, including passwords or access codes to business partner platforms or services, if a business partner platform has already been set out for your organization), online identifier, email address, account name, IP address, device identifiers or other similar identifiers.	To provide services you ask for, including operating and maintaining our Services, providing customer service and technical support. For quality, safety and internal research, including evaluating how our Services perform, repairing or improving the quality of our Services, tracking and responding to quality and security issues and developing new or enhanced products and service offerings. To promote and offer our Products, and those of our selected partners, through co-branded service offerings and joint marketing. To understand your preferences, make recommendations, and deliver personalized offers and communications.
Personal records, such as signature, telephone number or financial information.	To provide services you ask for, including operating and maintaining our Services, providing customer service and technical support. For quality, safety and internal research, including evaluating how our Services perform, repairing or improving the quality of our Services, tracking and responding to quality and security issues and developing new or enhanced products and service offerings. To promote and offer our Products, and those of our selected partners, through co-branded service offerings and joint marketing.
Demographic data/characteristics of protected classifications, including age, nationality and gender.	To provide services you ask for, including operating and maintaining our Services, providing customer service and technical support. For quality, safety and internal research, including evaluating how our Services perform, repairing or improving the quality of our Services, tracking and responding to quality and security issues and developing new or enhanced products and service offerings. To promote and offer our Products, and those of our selected partners, through co-branded service offerings and joint marketing.
Commercial information, including purchasing history.	To provide services you ask for, including operating and maintaining our Services, providing customer service and technical support. For quality, safety and internal research, including evaluating how our Services perform, repairing or improving the quality of our Services, tracking and responding to quality and security issues and developing new or enhanced products and service offerings. To promote and offer our Products, and those of our selected partners, through co-branded service offerings and joint marketing. To understand your preferences, make recommendations, and deliver personalized offers and communications.

Category of personal data	Purposes for collection, use and disclosure
Internet or other electronic network activity information, including how you interact with our Website, search history or other Website analytics information.	To provide services you ask for, including operating and maintaining our Services, providing customer service and technical support. For quality, safety and internal research, including evaluating how our Services perform, repairing or improving the quality of our Services, tracking and responding to quality and security issues and developing new or enhanced products and service offerings. To promote and offer our Products, and those of our selected partners, through co-branded service offerings and joint marketing. To understand your preferences, make recommendations, and deliver personalized offers and communications.
Geolocation data.	For quality, safety and internal research, including evaluating how our Services perform, repairing or improving the quality of our Services, tracking and responding to quality and security issues and developing new or enhanced products and service offerings. To understand your preferences, make recommendations, and deliver personalized offers and communications.
Sensory data, including audio, electronic, visual or similar information (e.g., photos, videos or recordings of you and your environment).	To provide services you ask for, including operating and maintaining our Services, providing customer service and technical support. For quality, safety and internal research, including evaluating how our Services perform, repairing or improving the quality of our Services, tracking and responding to quality and security issues and developing new or enhanced products and service offerings.
Professional or employment-related information.	To provide services you ask for, including providing customer service and scheduling demos.
Sensitive personal data, including information from government-issued identification (e.g., social security number, driver’s license, state identification card or passport number) and biometric information (e.g., faceprints, including facial mapping and scans of digitized images; and fingerprints, including scans of digitized images).	To provide services you ask for, including operating and maintaining our Products.

We may also collect, use or disclose all categories of personal data described above for other purposes authorized by applicable laws, including:

- To help prevent the loss of life or serious injury or to protect the personal safety of Incode personnel, users of our Services, visitors or the public;
- To detect, investigate, prevent or otherwise address fraud or other security and integrity issues;
- As part of a corporate transaction or proceeding such as a merger, financing, acquisition, bankruptcy, dissolution, or at transfer, divestiture or sale of all or a portion of our business or assets;
- To operate and maintain the security and integrity of our Services; and
- To protect our rights or property, our affiliates or others including by enforcing our agreements, terms and policies.

If you are a User of our Products, you will be able to voluntarily provide your personal data, including biometric information, to verify your identity, authenticate your information and prevent fraud when you use our Customers' websites or mobile applications. We collect your personal data through the photographic function in the applicable hardware, in each case when you initiate the capturing of a photograph, and/or when and if you manually include it.

Solely when we provide Incode Omni to our Customers, we may (as required by the Customer) disclose the personal data on your government-issued ID) and your biometric information (specifically, your faceprint) for the sole purpose of verifying your identity against the official source of your ID to obtain a YES/NO answer (i.e. you are or are not in the official database). As of the date of this Privacy Notice, we may share personal data with official sources in Mexico.

We may create aggregated data from the personal data we collect We may use such aggregated data and share it with third parties for our lawful business purposes, including to analyze, build and improve the Services and promote our business.

5. How does Incode disclose personal data?

We will not share opt-in consent or phone numbers with any affiliated businesses or third parties.

We may disclose your personal data to the categories of recipients listed in this section.

Service providers: These vendors help us provide the Services or perform business functions on our behalf. These vendors will only process your personal data for purposes described in this Privacy Notice. They include:

- Hosting, technology and communication providers.
- Security and fraud prevention consultants.
- Support and customer service vendors.

Please note that in connection with the Incode Omni and Incode ID services, we may disclose your personal data to vendors such as identity verification and fraud detection agencies to help us verify your identity, gather background information about you and protect our Customers against fraud. We do so solely at the direction and on behalf of our Customers and we do not retain any personal data we receive from such agencies for our own purposes. Please contact the relevant Customer if you have any questions about the disclosure of your personal data.

Analytics partners: These parties provide analytics on web traffic or usage of the Website. They include:

- Companies that track how users found or were referred to the Website.
- Companies that track how users use and interact with the Website.

Business partners: These parties collaborate with us in offering various services. They include:

- Businesses that you have a relationship with.
- Companies that we partner with to offer joint offerings or opportunities.

Legal obligations: We may disclose any personal data that we collect when required or permitted by law, such as to law enforcement agencies, courts, regulatory agencies and others, including to comply with valid legal process.

Business transfers: Your personal data may be transferred to a third party (and their agents and advisers) if we undergo a merger, acquisition, bankruptcy, financing, dissolution, transfer, divestiture, sale of all or a portion of our business or assets or other transaction in which that third party assumes control of our business (in whole or in part).

Consent: We may disclose your personal data with others if we have obtained your consent to such disclosure, including where you specifically authorize or direct us to disclose your personal data to our business partners.

6. Cookies and other similar technologies

Incode and our vendors may use cookies and other similar technologies, such as pixels, tags, web beacons and trackers (collectively, “Cookies”) on the Website. We may use Cookies for several purposes, including to:

- Store information to help the Website function properly,
- Help you access and navigate the Website more efficiently,
- Enable our servers to recognize your login information and preferences so that you do not need to enter the same information each time you visit the Website,
- Tell us how and when you visit and use our Services, including collecting information about which pages on our Website you viewed or links you clicked and how you interacted with our content during your visit or over multiple visits,
- Customizing your browsing experience by showing you information more likely to be relevant to you, and
- Delivering and customizing advertisements and tracking advertising campaigns.

We may use third-party technologies (such as the Meta Pixel and Hotjar) in connection with your activity on the Website, including for advertising purposes and to analyze your interactions and experiences with the Website, and including the features you engage with, how you navigate, and your click/touch, movement, scroll and keystroke activity. These technology companies and advertisers may use, store, or access cookies and other tracking technologies to collect or receive information from the Website and elsewhere on the internet. To change your privacy and advertising settings with Meta, log in to your Meta account and navigate to your account settings.

We may also use certain web analytics services, such as Google Analytics, to help analyze how people use our Website. We use this information to implement Google advertising features such as dynamic remarketing, interest-based advertising and demographics and interests reporting. For more information on how Google Analytics uses the data it collects, visit: google.com/policies/privacy/partners. To opt-out of Google Analytics, visit: tools.google.com/dlpage/gaoptout. To adjust your Google advertising settings, visit: adssettings.google.com.

You may be able to opt-out of certain interest-based advertising using the settings on your browser or mobile device. In addition, to opt-out of interest-based advertising from companies that participate in the Digital Advertising Alliance or European Interactive Digital Advertising Alliance opt-out programs, please visit: youradchoices.com/control and youronlinechoices.eu.

Please note that we or other parties may collect personal data about your online activities over time and across different devices and online websites when you use the Website.

Some browsers have incorporated “Do Not Track” (DNT) features that can send a signal to the websites you visit indicating you do not wish to be tracked. Because there is not a common understanding of how to interpret the DNT signal, our Website does not currently respond to browser DNT signals. Instead, you can use the range of tools described above to control data collection and use.

7. Your choices

You have the right to opt-out of marketing communications we send you at any time. You can stop receiving marketing communications by following the unsubscribe instructions in emails that you receive. To opt-out of other forms of marketing (such as postal marketing or telemarketing), then please email us at dataprotection@incode.com contact us using the contact details provided under the “Contact information” heading below.

8. Data security

We seek to protect your personal data from unauthorized access, use and disclosure using appropriate physical, technical, organizational and administrative security measures based on the type of personal data and how we are processing that personal data. You should also help protect your personal data by appropriately selecting and protecting your password and/or other sign-on mechanism; limiting access to your computer or device and browser; and signing off after you have finished accessing your account. Although we work to protect the security of your account and other personal data that we hold in our records, please be aware that no method of transmitting data over the internet or storing data is completely secure.

9. Data retention

We retain personal data about you for as long as necessary for the purpose(s) for which it has been collected and in accordance with applicable laws and regulations. For example, we will retain your personal data for as long as you have an open account with us or as otherwise necessary to provide you with our Services. In some cases we retain personal data for longer when we have an ongoing legitimate need to do so, (for example to comply with our legal, tax or accounting obligations, resolve disputes or collect fees owed), or where it is otherwise permitted or required by applicable law, rule or regulation. Because these needs can vary for different data types in the context of different services, actual retention periods can vary significantly based on criteria such as whether your personal data is reasonably necessary to manage our operations, to manage your relationship with us or to satisfy another purpose for which we collected the personal data; whether your personal data is reasonably necessary to carry out a disclosed purpose that is reasonably compatible with the context in which we collected the personal data; whether the personal data is reasonably required to protect or defend our rights or property; or whether we are otherwise required or permitted to keep your personal data by applicable laws or regulations (including, e.g., in Illinois (3years) and Texas (1 year). Where personal data is used for more than one purpose, we may retain it until the purpose with the latest period expires.

10. Personal data of children

We do not knowingly collect or solicit personal data about children under 18 years of age; if you are a child under the age of 18, please do not attempt to register for or otherwise use the Services or send us any personal data. If we learn we have collected personal data from a child under 18 years of age, we will delete that personal data in accordance with applicable law. If you believe that a child under 18 years of age may have provided personal data to us, please contact us at dataprotection@incode.com.

11. Additional information for Illinois residents

If you are an Illinois resident from whom we have collected biometric information, we may retain your biometric information only until the first of the following occurs, unless otherwise required by law or our contracts with Customers: (i) the initial purpose for collecting such biometric information has been satisfied; or (ii) 3 years after your last interaction with the Incode Omnior Incode ID, in accordance with Illinois law.

12. Additional information for California residents

If you are a California resident that uses our Products or interact with us in an individual or household capacity, the following information also applies to you and supplements the information contained in this Privacy Notice. In the event of any conflict between this section and our Privacy Notice above, this section shall govern for California residents.

References to "personal data" in this section are equivalent to "personal information" as defined by California law.

A. The California Consumer Privacy Act ("CCPA")

Your privacy rights. Under the CCPA, California residents have the following rights:

- **Right to Access/Know:** You have the right to request that we disclose to you the following personal data:
  - The categories and specific pieces of personal data we have collected about you in the last 12 months.
  - The categories of sources from which we collect personal data.
  - The business or commercial purposes for collecting, using, sharing or selling personal data.
  - The categories of personal data we have disclosed about you for a business purpose and the categories of recipients to which it was disclosed.
  - The categories of personal data we sold or shared about you and the categories of third parties to which each category of personal data was sold or shared.
- **Right to Delete:** You have the right to request that we delete your personal data that we have collected from you, subject to certain exceptions.
- **Right to Correct:** You have the right to request that we correct any inaccurate personal data we have collected about you. We may request documentation from you in connection with your request. Upon receipt of a verifiable request to correct inaccurate personal data, we will use commercially reasonable efforts to correct the personal data.
- **Your Opt-Out Rights:** We sell and share personal data for valuable consideration (not in exchange for money). This personal data is primarily collected via our use of Cookies. We share this personal data with our advertising partners and analytics vendors to assist with our cross-context behavioral advertising efforts. We sell and share the following categories of personal data described in Section 4 above:
  - Identifiers,
  - Internet or other electronic network activity information, and
  - Geolocation data.
- You may opt out of the sale and sharing of your personal data via Cookies through our Cookie preference center by clicking on the "Do Not Sell or Share My Personal Information" link in the footer of our Website. Right to Non-Discrimination: We will not discriminate against you for exercising any of these rights.
- **Exercising your rights.** To exercise the rights to access/know, delete, and/or correct, you or an agent you authorize to act on your behalf must send us a request that (1) provides sufficient information to allow us to verify that you are the person about whom we have collected personal data, and (2) describes your request in sufficient detail to allow us to understand, evaluate and respond to it. We may not respond to requests that do not meet these criteria. We will only use personal data provided in a request to verify your identity and complete your request. You do not need an account with Incode to submit a request.

We will work to respond to your valid request within 45 days of receipt. We will not charge you a fee for making a request unless your request is excessive, repetitive or manifestly unfounded.

You may submit a request using the following methods:

Call us at: +1 650 446 3444
Email us at: dataprotection@incode.com

Note that you must provide your authorized agent with written permission to exercise your rights on your behalf, and we may request a copy of this written permission from your authorized agent when they make a request on your behalf.

B. California Shine the Light Law

California law permits customers in California to request certain details about how their personal data is shared with third parties, and in some cases affiliates, if personal data is shared for those third parties' or affiliates' own direct marketing purposes. We do not share personal data with third parties or affiliates for those third parties' or affiliates' own direct marketing purposes. Californians may request information about our personal data sharing by contacting us at dataprotection@incode.com or by sending a letter to:

Incode Technologies, Inc.
101 Mission Street, Suite 900
San Francisco, CA 94105

Any such request must include your name and “California Shine the Light Privacy Rights Request” in the first line of the description and, if sent by mail, must include your street address, city, state, and zip code.

Please note that “Shine the Light” rights and CCPA rights are granted by different laws and must be exercised separately.

13. Additional information for Nevada residents

If you are a resident of Nevada, you have the right to opt out of the sale of certain personal data to third parties. You can exercise this right by contacting us at dataprotection@incode.com with the subject line "Nevada Do Not Sell Request" and providing us with your name and the email address associated with your account. Please note that we do not currently sell your personal data as sales are defined in Nevada Revised Statutes Chapter 603A.

14. Additional information for European residents

If you are a resident of the European Union ("EU"), United Kingdom ("UK"), Lichtenstein, Switzerland, Norway or Iceland, you may have additional rights under the EU General Data Protection Regulation (the "GDPR"), the UK GDPR and other European privacy laws with respect to your personal data, as outlined below. If there are any conflicts between this this section and any other provision of this Privacy Notice, this section shall govern for European residents. If you have any questions about this section or whether any of the following applies to you, please contact us at dataprotection@incode.com.

If you are a resident in the European Economic Area ("EEA"), UK or Switzerland, the controller of your personal data (excluding the processing performed on behalf of our Customers) is Incode Technologies, Inc.

A. Legal basis for processing personal data

We will only process your personal data if we have a legal basis for doing so. The legal basis on which we rely depend on the personal data concerned and the specific context in which we collect it. Generally, we rely on the following legal bases:

Contractual Necessity: We process your personal data as a matter of "contractual necessity," meaning that we need to process the data to perform a contract with you, such as to provide you with the Services through our Customers' applications and/or websites. When we process personal data due to contractual necessity, failure to provide such personal data will result in your inability to use some or all portions of the Services that require such personal data.

Legitimate Interest: We may also process your personal data when we believe it furthers the legitimate interest of us or other parties and such interest is not overridden by your data protection interests or fundamental rights and freedoms. Examples of these legitimate interests include:

- Providing, customizing and improving the Services;
- Corresponding with you;

- Promoting our Services; and
- Maintaining the security of our Services.

We may have other legitimate interests and if applicable, we will make clear to you at the relevant time what those legitimate interests are.

Consent: In some cases, we process personal data based on the consent you expressly grant to us at the time we collect such personal data. When we process personal data based on your consent, it will be expressly indicated to you at the point and time of collection.

Legal Obligation: From time to time we may also need to process personal data to comply with a legal obligation, if it is necessary to protect the vital interests of you or other data subjects, or if it is necessary for a task carried out in the public interest.

B. European data subject rights

European residents have certain rights with respect to your personal data, including those set forth below. For more information about these rights, or to submit a request, please email us at dataprotection@incode.com. Please note that we will respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws. In some cases, we may also need you to provide us with additional information, which may include personal data, if necessary to verify your identity and the nature of your request.

- **Access:** You can request more information about the personal data we hold about you and request a copy of such personal data.
- **Portability:** You can ask for a copy of your personal data in a machine-readable format. You can also request that we transmit the data to another controller where technically feasible.
- **Rectification:** If you believe that any personal data we are holding about you is incorrect or incomplete, you can request that we correct or supplement such personal data.
- **Erasure:** You can request that we erase some or all of your personal data from our systems.
- **Restriction of Processing:** You can ask us to restrict further processing of your personal data.
- **Objection:** You can contact us to let us know that you object to the further use or disclosure of your personal data for certain purposes, such as for direct marketing purposes.
- **Withdrawal of Consent:** If we are processing your personal data based on your consent (as indicated at the time of collection of such personal data), you have the right to withdraw your consent at any time. Please note, however, that if you exercise this right, it will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal data conducted in reliance on lawful processing grounds other than consent.

- You have the right to lodge a complaint about Incode's practices with respect to your personal data with a supervisory authority, in particular, in the Member State of your habitual residence, place of work or place of the alleged infringement. A list of Supervisory Authorities is available here: https://edpb.europa.eu/about-edpb/board/members_en.

C. Transfers of personal data

Incode is a United States company with service providers located in the United States and other countries. This means that your personal data may be transferred to, and processed in, countries other than the country in which you are located. These countries may have data protection laws that are different to the laws of your country (and, in some cases, may not be as protective). We take appropriate safeguards to ensure that your personal data remains protected in accordance with this Privacy Notice and applicable data protection laws. If you are located in the EEA, UK or Switzerland, these safeguards include transferring your personal data to a country that applicable authorities have determined provides an adequate level of protection for personal data, or by implementing the Standard Contractual Clauses with our Customers, service providers and partners. If you wish to obtain a copy of our Standard Contractual Clauses, please contact us by sending an email to dataprotection@incode.com. By accessing and/or using our Services, you agree to the processing of your personal data in the jurisdiction in which we operate.

15. Additional information for Australian residents

If you reside in Australia or are using our services or interacting with Incode in Australia, the following applies to you. This section supplements, supersedes and extends the scope of this Privacy Notice generally. The remaining sections of this Privacy Notice, other than those sections which are expressly limited to foreign jurisdictions outside of Australia or are inconsistent with the specifics of this section, also apply to you and you should consider this Privacy Notice in full for full details of how we manage your personal data, including the kinds of personal data we collect, how we collect your personal data and the purposes for which your personal data is collected, held, used and disclosed.

A. Are we a data controller or data processor?

Some privacy regimes that we are subject to distinguish how we may collect, use and disclose your personal data depending on whether we are classified as a "data processor" or "data controller." Under these regimes, we act as a processor when providing identity verification services to our Customers. The "data processor" and "data controller" distinction is not relevant to you to the extent Australian privacy law applies and we have obligations to you with respect the personal data we hold about you, even when acting as a "data processor." The "data processor" section below explains how we collect and process personal data as data processors on behalf of our Customers in the course of providing our Services. However, these practices are dependent on, and connected with, the data collection and use practices of our Customers.

B. Information we collect as a Data Processor

In certain instances where you use the Incode Omni, we are acting as a data processor on behalf of our Customers for the purposes of certain applicable privacy laws. In these circumstances, there is no difference in the manner of how we collect your personal data, the type of personal data collected or the third parties to whom we may disclose personal data collected to. You should refer to the sections titled “What personal data does Incode collect and why does Incode collect it?” and “How does Incode disclose personal data?” for information regarding what personal data we collect and how we collect and disclose personal data, respectively, when acting as data processors on behalf of our Customers.

The purpose for which we collect your personal data when using Incode Omni remains to verify your identity, authenticate your information and prevent fraud when you use our Customers’ websites or mobile applications. When we act as data processors, exactly how and to what extent Incode Omni is applied or operated may be subject to our Customer’s instructions or control. When acting as a data processor, the personal data that you input into Incode Omni may also be collected by, or held at the direction of, our Customers. Our Customers will use and disclose such personal data in accordance with their own privacy practices and obligations and in accordance with applicable law. We invite you to contact or refer to the relevant Customer if you need any further information regarding the privacy practices of our Customers.

While your use of Incode Omni is always voluntary and subject to your consent, we note that our Customers may be required by law to verify your identity to certain prescribed standards prior to offering services to you. For further information regarding your personal data in those cases beyond the details herein included regarding Incode’s activity, we invite you to contact the relevant company or organization if you have any questions about their privacy practices. In all other cases, we act as a data controller of your personal data for the purposes of applicable privacy law.

C. Your rights under Australian privacy law

You are entitled to access the personal data we hold about you and may request that we correct any errors in the personal data we hold. If you would like to access or correct your personal data held by us, please contact us at:

- dataprotection@incode.com
- Australia Square
- Level 33, 264 George Street
- Sydney, NSW 2000.

We will take reasonable steps to allow you to access your personal data unless reasonable circumstances exist that would prohibit us from doing so.

We will correct your personal data where we are satisfied that the personal data is inaccurate, out of date, incomplete, irrelevant or misleading. If we correct any personal data that we have disclosed to third parties we will take reasonable steps to notify those parties of the change or update. You accept that, following a request to correct your personal data, we may be required to take reasonable steps to verify your identity or the personal data, which may include confirmation with third parties.

If you are concerned that we may have breached the Australian Privacy Principles, please contact us immediately at the contact details set out above. We will undertake a reasonable and expeditious assessment of the concern and suggest relevant resolution processes. This process will be completed as soon as practicable and in any event within 30 days. If you are unsatisfied with our response to, or resolution of, your complaint you may choose to contact the Office of the Australian Information Commissioner at their website www.oaic.gov.au.

D. Direct marketing in Australia

Where we use your personal data to send you marketing and promotional information you will be provided with the opportunity to opt-out of receiving such information. Unless you exercise your right to opt-out of such communication, you will be taken to have consented to receive similar information and communications in the future.

16. Changes to this Privacy Notice

We may update this Privacy Notice from time to time, and, in some cases, we may provide you with additional notice at our discretion. You can see when this Privacy Notice was last updated by checking the “Last Modified” date displayed at the top of this Privacy Notice.

17. Contact information

If you have any questions or comments about this Privacy Notice, the ways in which we collect and use your personal data or your choices and rights regarding such collection and use, please do not hesitate to contact us at:

- **Tel**: +1 650 446 3444
- **Email:** dataprotection@incode.com

- **Mail**: Incode Technologies, Inc., 101 Mission Street, Suite 900, San Francisco, CA 94105