Data Processing Addendum

Last revised February 2023

This Data Processing Addendum, including its Appendices, (the "DPA") forms part of the Cloud Services Agreement ("Agreement") by and between Nametag, Inc. ("Nametag" or "Company") and Customer (as defined in the Agreement), (each a "Party" and collectively the "Parties"), pursuant to which Nametag provides the services to Customer as described in the Agreement (the "Services"). The Parties agree that references to Customer in this DPA include Customer and its Affiliates. This DPA is effective when signed or otherwise agreed to by the Parties (the "Effective Date") and shall apply for the duration of the Agreement and for as long as Nametag and/or Sub-processor(s) Processes Personal Information.

This DPA is also incorporated into Nametag's End User License Agreement and applies to End Users in the European Economic Area, United Kingdom, or Switzerland, or otherwise subject to the General Data Protection Regulation ("GDPR").

This DPA supplements the Agreement by setting out the agreement between the Parties for Nametag's Processing of Personal Information to protect and safeguard Customer's Personal Information, in accordance with Applicable Data Protection Law. All capitalized terms in this DPA shall have the meaning set forth in this DPA. Capitalized terms not otherwise defined in this DPA will have the meaning given to them in the Agreement, or if not defined in the Agreement, by Applicable Data Protection Law.

Except as specifically set forth in this DPA, all of the terms and provisions of the Agreement shall remain unmodified and in full force and effect. In the event of any conflict between the Agreement and this DPA, the terms of this DPA will prevail. If a provision of this DPA is or becomes ineffective in whole or in part due to applicable law or regulatory action, or if there is an omission of terms or provisions required by appliable law, the remaining provisions of this DPA shall remain unaffected. In place of the ineffective provisions, and/or to remedy an omission, the parties will discuss and negotiate in good faith to agree to reasonable terms or provisions which come, to the extent legally possible, closest to the parties' original intentions and applicable legal requirements.

In the event that a change in any Applicable Data Protection Law, or as provided for by a data protection authority or regulator, results in the transfer or processing of Personal Information under this DPA no longer being lawful or otherwise permitted, the parties agree to remediate the processing (by amendment to this DPA or otherwise) to the extent practical to meet the necessary standards or requirements and, if necessary, amend the DPA as set forth above.

1. Definitions

1.1 "Affiliates" means any entity which directly or indirectly controls, is controlled by, or is under common control with a party to the Agreement or this DPA. For purposes of this definition, control means direct or indirect ownership or control of more than 50% of the voting interest of the subject entity.

1.2 "Applicable Data Protection Law" means all data protection and privacy laws applicable to the processing of Personal Information under the Agreement, including, where applicable: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR") and any data protection laws in any EU or EEA Member State including laws implementing such Regulation, (ii) the GDPR as incorporated into United Kingdom ("UK") law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 ("UK GDPR"); (iii) the Federal Act on Data Protection of June 19, 1992 (DPA) of Switzerland and its ordinances ("Swiss FADP"); and (iv) the California Consumer Privacy Act of 2018 ("CCPA"), including as each may be replaced, revised or amended from time to time.

1.3 "Controller" means 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 Information, including a "controller" as such term is defined by the GDPR, a "business" as such term is defined by the CCPA, or a similar designation under and regulated by Applicable Data Protection Law.

1.4 "Customer" means the Customer legal entity who has entered into the Agreement with Nametag.

1.5 "Customer Data" means non-public information, including any Personal Information, provided by Customer to Company under the Agreement in order to receive the Services. and may include End User Information.

1.6 "Data Subject" means an identified, or identifiable, natural person to whom Personal Information relates, or who is otherwise a "data subject" as such term is defined by the GDPR, a "consumer" as such term is defined by the CCPA, or a similar designation under and regulated by Applicable Data Protection Law.

1.7 "EEA" means the European Economic Area.

1.8 "End User" means a real person about whom Customer requests Personal Information from Company using the Services. End Users' use of the Services is governed by the EULA.

1.9 "End User Information" means information and common data, including any Personal Information, provided by an End User to Company in connection with their use of the Services (e.g., scans of government IDs, etc.). Where an End User provides their End User Information directly to Company, the End User is the Controller and Company is the Processor for purposes of this DPA.

1.10 "End User License Agreement" (or "EULA") means the End User License Agreement that sets forth the terms of service governing each End User's use of the SaaS Services, and available at https://getnametag.com/legal/eula.

1.11 "Instructions" means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Information (including,

but not limited to, depersonalizing, blocking, deletion, making available), as may be amended or updated from time to time.

1.12 "Personal Information" means (i) any information relating to an identified or identifiable individual, or (ii) is otherwise "Personal Data" as such term is defined by the GDPR or UK GDPR, "Personal Information" as such term is defined by the CCPA, or a similar designation under and regulated by Applicable Data Protection Law.

1.13 "Personal Information Breach" means accidental, unauthorized or unlawful destruction, damage, loss, alteration, encryption, access (including unauthorized internal access), disclosure, acquisition or use of Personal Information, or any loss of control over Personal Information (including unauthorized encryption of Personal Information via ransomware or other means), stored or otherwise Processed by Nametag and/or Nametag's Sub-processors.

1.14 "Processing" (and its cognates) means any operation or set of operations which is performed on Personal Information or sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, modification, disclosure, dissemination, making available, alignment or combination, restriction, erasure or destruction. The terms "Process", "Processes", and "Processed" will be construed accordingly.

1.15 "Processor" means a natural or legal person, public authority, agency, or other body which Processes Personal Information on behalf of the Controller subject to contractual restrictions consistent and in compliance with Applicable Data Protection Law, including a "processor" as such term is defined by the GDPR, a "service provider" as such term is defined by the CCPA, or a similar designation under and regulated by Applicable Data Protection Law.

1.16 "Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of Personal Information, in accordance with Applicable Data Protection Law, to Controllers and Processors established in Third Countries, the approved version of which is in force at the date of signature of the Agreement that are in the European Commission's Decision 2021/914 of 4 June 2021 (referencing Module Two: Transfer Controller to Processor, and/or other modules as applicable), and as may be amended or replaced by the European Commission from time to time.

1.17 "Sub-processor" means any Processor engaged by the Nametag or its Affiliates who Processes any Personal Information on behalf of the Nametag.

1.18 "UK Transfer Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office (Version B1.0, in force as of 21 March 2022).

2. Description of Personal Information; Instructions for Processing

Customer as the Controller (or as a Processor for another Controller) appoints Nametag as a Processor (or Sub-Processor) to Process Personal Information in connection with the services provided under the Agreement. The categories of Personal Information, the categories of Data Subjects, and the types of

Processing are outlined in Appendix 1. The parties agree that the DPA and the Agreement constitute Customer's Instructions to Nametag in relation to the Processing of Personal Information, and Nametag agrees to process Personal Information in accordance with its Instructions.

3. Controller Obligations

Customer represents and warrants that: (1) its Processing instructions will comply with all Applicable Data Protection Law; and (2) it has obtained and maintains all legally required notices, consents and permissions for the Processing and transfers of all Customer Information.

4. Processor Obligations

Nametag represents and warrants that it will only Process Personal Information on Customer's documented Instructions and only for the purposes of providing the Services incorporated in this DPA and the Agreement to Customer (the "Permitted Purpose") or as otherwise agreed within the scope of Customer's lawful Instructions, except where and to the extent otherwise required by Applicable Data Protection Law. Nametag further represents and warrants that its Processing of Personal Information will comply with Applicable Data Protection Law.

If required by Applicable Data Protection Law to Process Personal Information for a purpose other than the Permitted Purpose or if Nametag becomes aware that Nametag cannot Process Personal Information in accordance with Customer's Instructions due to a legal requirement under any applicable law, Nametag shall (i) promptly notify Customer of such legal requirement in writing and (ii) Customer may, in its sole discretion, request Nametag cease all Processing (other than merely storing and maintaining the security of the affected Personal Information) of Personal Information until such time as Customer issues new Instructions to Nametag. If a performed instruction is subsequently found to be in violation of Applicable Data Protection Law, such violation will not constitute Nametag's breach of this DPA or Applicable Data Protection Law.

Nametag will promptly inform Customer where Nametag receives any request for access to or disclosure of the Personal Information by a law enforcement, judicial, regulatory or other governmental authority ("Disclosure Request"). Nametag shall take the following measures: (i) Nametag will promptly notify Customer of the Disclosure Request sufficient to allow Customer to object to the request and/or seek a protective order, unless Nametag is explicitly prohibited from doing so by law, court order or other legal requirement, or the circumstances otherwise preclude such notification; (ii) Nametag will refer the Disclosure Request to Customer and provide reasonable assistance to Customer in opposing such disclosure or seeking a protective order, unless Nametag is explicitly prohibited from doing so by law, court order or other legal requirement; (iii) Nametag shall only provide information when and to the extent legally required to do so; and (iv) where Nametag is legally compelled, Nametag shall disclose the minimum amount of information required to be disclosed by law.

Nametag acknowledges that Customer may disclose this DPA and any relevant data protection provisions in the Agreement as necessary to meet Customer's obligations under Applicable Data Protection Law or pursuant to a request by a law enforcement, judicial, regulatory or other governmental authority with jurisdiction over the parties, this DPA, or the Agreement.

To the extent Customer discloses Personal Information of California consumers or households, Nametag may be considered a “service provider” as defined in CCPA Section 1798.140(v), as applicable. Nametag acknowledges and agrees that Customer discloses Personal Information to Nametag solely for: (i) a valid business purpose; and (ii) Nametag to perform the Services as set forth in the Agreement. Nametag is prohibited from: (i) selling Personal Information; (ii) retaining, using, or disclosing Personal Information for a commercial purpose other than providing the Services to Customer; (iii) retaining, using, or disclosing the Personal Information outside of the direct business relationship between Nametag and Customer; or (iv) using the Personal Information to provide services to another person or entity. Nametag hereby certifies it understands and will comply with these obligations and restrictions in accordance with the CCPA. Furthermore, Nametag agrees to reasonably assist Customer in responding to any requests from a California consumer or household exercising their rights under the CCPA.

5. Confidentiality

In addition to the confidentiality provisions of the Agreement (if applicable), Nametag will ensure that any personnel that processes Personal Information on its behalf, including without limitation Nametag’s employees, subcontractors or other authorized personnel ("Authorized Persons") are subject to a duty of confidentiality (whether a contractual duty or a statutory duty), and Nametag shall not permit any person to Process the Personal Information who is not under such a duty of confidentiality. Nametag shall ensure that all Authorized Persons Process the Personal Information only as necessary for the Permitted Purpose.

6. Technical and Organizational Measures

Nametag shall implement and maintain for the duration in which Nametag holds or otherwise Processes Personal Information, appropriate technical and organizational measures to ensure a level of security required to protect Personal Information, including from any actual loss, from any unauthorized or unlawful Processing, and from any Personal Information Breach.

The technical and organizational measures required by this section shall include the measures set out in Appendix 2 (“Security Measures”). Nametag may modify or update the Security Measures provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

Customer acknowledges and agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

7. Sub-processors

Nametag and Customer agree that Nametag may engage Sub-processors to Process Personal Information on Customer’s behalf subject to the terms of this DPA. Nametag has currently appointed, as Sub-processors, the third parties listed in Appendix 3 to this DPA. Nametag shall provide no less than 30 days prior notice to Customer regarding proposed new or replacement Sub-processors during the term of the Agreement. If Customer reasonably objects in writing to a new or replacement Sub-processor within 10

calendar days after receipt of such notice, and the parties cannot resolve Customer's reasonable objection within 14 calendar days after receipt of such objection, then Customer may terminate the Services impacted by the new or replacement Sub-processor on written notice to Nametag without penalty and receive a pro-rata refund of any fees paid in advance.

In the event that Nametag engages a Sub-processor to assist with or carry out the Processing activity on its behalf, Nametag will impose data protection terms on the Sub-processors providing at least the same level of protection for the Personal Information and the rights of Data Subjects as required in the Agreement and this DPA, and that at a minimum, provide data protection, security, and confidentiality obligations no less strict as set out in this DPA and Agreement. Nametag shall remain fully liable to Customer for each Sub-processor's compliance with the obligations of this DPA, the Agreement, and Applicable Data Protection Law, and for any acts or omissions of such Sub-processor that cause Nametag to breach any of its obligations under this DPA and the Agreement.

Notwithstanding the foregoing, Nametag may replace or add a Sub-processor without prior notice to Customer if, in its sole discretion, such action is necessary to prevent or mitigate risk to the Services, Personal Information, technology infrastructure, or Nametag's other customers. Nametag shall notify Customer of the replacement or additional Sub-processor as soon as reasonably possible, and Customer shall retain the right to object to such Sub-processor as described herein upon receipt of such notice.

8. Location of Processing; Cross-Border Transfers

All Personal Information will be stored and processed in the countries set forth in this DPA and will not be transported to or Processed and stored in any third country without the Customer's or End User's prior written consent. Personal Information received from Customers or End Users in Asia, North America or South America will be stored and Processed in the United States. Personal Information received from Customers or End Users in Europe or Africa will be stored and Processed in Ireland or Germany. From time to time, Company may add additional regional data centers and will provide written notice to Customer or End User of the same.

To the extent Nametag's Processing of Customer Data and/or End User Information includes Personal Information of Data Subjects in the EEA, Switzerland and/or UK, Customer and Nametag acknowledge and agree that such Personal Information may be transferred to third countries, including countries that are not recognized by the European Commission, UK or Switzerland as providing an adequate level of protection for Personal Information. More specifically, Customer and End User acknowledge and agree that Personal Information may be transferred to Nametag in the United States, which has not received an adequacy determination. Customer and End User hereby consents to the transfer of Personal Information to Nametag in the United States as set forth herein. For such cross-border transfers, Customer or End User is the Data Exporter and Nametag is the Data Importer.

For Personal Information of Data Subjects in the EEA, the Standard Contractual Clauses are implemented as follows:

- Clause 7, the "Docking Clause (Optional)", shall be deemed incorporated;
- In Clause 9, the parties choose Option 1, Specific Authorization, with a time period of 30 days;

- The optional wording in Clause 11 shall be deemed not incorporated;
- Clause 17 and Clause 18, the governing law and forum shall be the Republic of Ireland; and
- Appendixes 1, 2 and 3 attached hereto serve as Annexes I, II and III of the Standard Contractual Clauses.

For Personal Information of Data Subjects in Switzerland, the Standard Contractual Clauses (as revised herein) are implemented as follows:

- The Swiss Federal Data Protection and Information Commissioner shall be the sole Supervisory Authority for the transfers exclusively subject to the Swiss FADP;
- The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the Standard Contractual Clauses shall be interpreted to include the Swiss FADP with respect to the transfers;
- References to Regulation (EU) 2018/1725 are removed;
- References to the "Union", "EU" and "EU Member State" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses;
- Where the transfers are exclusively subject to the Swiss FADP, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the Swiss FADP; and
- Where the transfers are subject to both the Swiss FADP and the GDPR, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the Swiss FADP insofar as the transfers are subject to the Swiss FADP.

For Personal Information of Data Subjects in the UK, the UK Transfer Addendum is implemented as follows:

A. Table 1: Parties

- The Start Date is the effective date of the Agreement.
- The Customer's and Nametag's details and key contacts are provided in the Agreement.
- The parties' signatures on the Agreement constitute their signatures for purpose of this UK Transfer Addendum.

B. Table 2: Selected SCCs, Modules and Selected Clauses

The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this UK Transfer Addendum:

- Module in operation: Module 2: Transfers Controller to Processor or (Module 3: Transfers Processor to Processor), as applicable
- Clause 7 (docking clause): Yes.
- Clause 9: Specific authorization and 30 days.
- Clause 11 (option): No

C. Table 3: Appendix Information

- Annex IA: The list of parties (Customer and Nametag) is provided in the Agreement.
- Annex IB: Description of Transfer: A description of the transfer is provided in Appendix 1 of this Data Processing Addendum.
- Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Nametag's implemented security measures are described in Appendix 2 of this Data Processing Addendum.
- Annex III: Nametag's list of Sub-processors is provided in Appendix 3 of this Data Processing Addendum.

D. Table 4: Ending this UK Transfer Addendum when the Approved Addendum Changes

Either Customer or End User or Nametag can end this UK Transfer Addendum as set out in Section 19 of the UK Transfer Addendum.

The parties further agree that if the Standard Contractual Clauses or the UK Transfer Addendum are updated, replaced or are no longer available for any reason, the parties will cooperate in good faith to implement updated or replacement Standard Contractual Clauses or UK Transfer Addendum, as appropriate, or identify an alternative mechanism(s) to authorize the contemplated cross-border transfers.

9. Personal Information Breach

Nametag will notify Customer without undue delay upon becoming aware of a Personal Information Breach, or facts sufficient to form a reasonable suspicion that a Personal Information Breach has occurred or will occur, in relation to Personal Information transmitted, stored, or otherwise Processed by Nametag or its Sub-processors. Nametag's notice does not constitute an admission of fault by Nametag or its Sub-processors for the actual or potential Personal Information Breach. Nametag shall reasonably cooperate and provide timely information regarding the Personal Information Breach as it becomes known and is requested by Customer and also assist in the investigation of any such actual or potential Personal Information Breach. Except to the extent required by Applicable Data Protection Law, Nametag will not make any statement or notification to any Data Subject, customer, regulator, or otherwise relating to such Personal Information Breach as it relates to Personal Information without the prior written approval of Customer in each instance.

10. Deletion or Return of Personal Information

Except as otherwise provided below, Nametag shall delete or return Personal Information of Customers and End Users (including without limitation any copies thereof and any Personal Information subcontracted to a Sub-processor for Processing) (i) on termination or expiration of the Agreement or this DPA or (ii) upon request by Customer, save that this requirement shall not apply to the extent that Nametag is required by Applicable Data Protection Law to retain some or all of the Personal Information, in which event Nametag shall isolate and protect that Personal Information from any further Processing except to the extent required by such law. Upon request by Customer, Nametag shall provide evidence of

such deletion or return of Personal Information, including without limitation written confirmation of such deletion or return.

Nametag's obligation to delete or return Personal Information of End Users applies only to Personal Information, including End User Information, that End Users consented to share exclusively with or collected by Customer. Personal Information, including End User Information, that End Users shared with other customers of Nametag or shared with Nametag is not subject to deletion or return to Customer pursuant to this Section 10.

11. Information Requests and Audit Rights

Nametag shall make available to Customer all information necessary and reasonably requested by Customer to demonstrate compliance with the obligations set forth in this DPA and, at Customer's expense, allow for and contribute to audits, including inspections, conducted by the Customer or an independent third-party auditor mandated by the Customer. Any such audits or inspections shall be limited to once in any rolling 12-month period unless ordered by a supervisory authority or other competent legal authority or upon the occurrence of a Personal Information Breach. If the requested audit scope is addressed in an SSAE 16/ISAE 3402 Type 2, ISO, NIST or similar data security audit report performed by a qualified third-party auditor ("Audit Reports") within twelve (12) months of Customer's audit request and Nametag confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

***

APPENDIX 1: DESCRIPTION OF THE TRANSFER

Appendix 1(A): List of parties	
Data exporter	**Name of the data exporter: Customer or End User as identified in the Agreement or EULA, respectively** **Contact person's name, position and contact details: Contact identified in the Agreement or EULA** **Address: Address provided in the Agreement or EULA** **Activities relevant to the data transferred: transfer of Personal Information to Nametag for the purposes of providing the Services as more particularly described in the Agreement** **Role (Controller/Processor): Controller**
Data importer	**Name of the data importer: Nametag Inc.** **Contact person's name, position and contact details: Ross Kinder, CTO, privacy@nametag.co** **Activities relevant to the data transferred: Nametag's Processing of Personal Information on behalf of Customer for the purposes of providing the Services as more particularly described in the Agreement** **Address: 520 East Denny Way, Seattle, WA 98122 USA** **Role (Controller/Processor): Processor**
Appendix 1(B): Description of the transfer	
Description of transfer	**Categories of Data Subjects whose Personal Information is transferred:** ● **Customer's employees and other authorized representatives accessing and using the Services** ● **End Users whose identity is to be authenticated using the Services** **Categories of Personal Information transferred:** ● **Name, email address, telephone number of Customer's employees and other authorized representatives accessing and using the Services** ● **Name and email address generated by Nametag and any other Personal Data that an End User may consent to share with data exporter** **Sensitive Data transferred (if appropriate) and applied restrictions or safeguards:** **Biometric information for identify verification (applicable security measures set forth in Appendix 2)**

	Frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis): **Continuous** **Nature and subject matter of the Processing:** **Identity services for authentication and account recovery** **Duration of the Processing:** **Nametag will Process Personal Information for the duration of the provisioning of the Services and in accordance with the Agreement or EULA** **Purpose of the data transfer and further Processing:** **To enable Nametag to provide the Services in accordance with the Agreement or EULA** **Period for which the Personal Information will be retained, or if that is not possible the criteria used to determinate that period:** **Nametag will retain the Personal Information for the duration of the Services and in accordance with the Agreement or EULA** **For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:** **The subject matter and nature of transfers to sub-processors identified in Appendix 3 are to support Nametag's provisioning of the Services to Customer or End User. The duration of transfers is same as the duration of the processing by Nametag.**
Appendix 1(C): Competent supervisory authority	
Competent supervisory authority	**The data protection authority of the EEA member state in which Customer or its Affiliate has entered into the Agreement is established or, if Customer or its Affiliate is not established in the EEA, the Irish Data Protection Commissioner. For the purposes of UK and Swiss transfers, the competent supervisory authority is the UK Information Commissioner's Office or Swiss Federal Data Protection Information Commissioner (as applicable).**

APPENDIX 2: SECURITY MEASURES

Description of the technical and organizational measures implemented by Nametag (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of natural persons.

The following is a description of the technical and organizational measures implemented by Nametag (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of natural persons,

Introduction

Nametag is a SaaS identity platform that provides validated identity on the web, in person, and over the phone with a low-friction enrollment process that positively validates people using their US government-issued identification and facial recognition. The person authenticated by the identification retains control over who is using their information, while the company or person using their information has no need to store PII. Everyone—people and companies—is more secure using Nametag.

To provide this, we must make sure that your sensitive data is secure, and protecting it is our most important responsibility. We're committed to being transparent about our security practices and helping you understand our approach.

Infrastructure

Our service is hosted on infrastructure operated by Amazon Web Services (AWS) (Learn More).

AWS is Amazon's global scale technical infrastructure designed to provide security through the entire information processing lifecycle. This infrastructure provides secure deployment of services, secure storage of data with end user privacy safeguards, secure communications between services, secure and private communication with customers over the internet, and safe operation by administrators.

The security of the infrastructure is designed in progressive layers starting from the physical security of data centers, continuing on to the security of the hardware and software that underlie the infrastructure, and finally, the technical constraints and processes in place to support the operational security of data stored with Nametag.

AWS invests heavily in securing its infrastructure with many hundreds of engineers dedicated to security and privacy.

Data Encryption

Nametag handles data in these contexts:

- **at rest on your phone in our app (there is no permanent storage in the app, but we do use the app to send and receive data for enrollment, sharing requests, and display purposes).**
- **Over the public Internet from your phone to the Nametag services in AWS.**
- **at rest in AWS storage (databases and object storage buckets).**
- **from Nametag services in AWS to people with whom you share your data—either another user's Nametag app, or a website that requires authenticated data about you, or someone on the phone confirming your identity.**

In the cases of our app and the Nametag services and storage within AWS, the data is encrypted at rest and in transit. In the cases of a third-party website or voice verification, please refer to that third-party's security documentation.

For some functions, we must manage secrets on your behalf. For example, in order to implement OAuth, we create keys that authenticate your application for information access. Wherever we check access to a resource, for example access to our API or when our app communicates with our services, we either store those secrets using a one-way hash (bcrypt2) or authenticate them with a digital signature (ECDSA with a P-256 key)

Secure Deployment

The Nametag source code is stored in a central code repository. Making changes to the software requires the review and approval of at least one other member of the team. Our software infrastructure is short-lived and deployed in its entirety on a regular basis. Rather than modify running systems, we destroy and replace systems to deploy new versions.

Because deployments are automated, it is unusual for staff to access the production environment directly. This access is extremely rare and limited to key personnel. All such access is audited and recorded.

Security Vulnerabilities

We have made architectural choices that make vulnerabilities more difficult to introduce. For example, the identity and privilege level of the remote user is threaded throughout the application, all the way to the datastore, which enforces access rules in a testable, auditable place. The peer-code review process serves as a backstop against intentional or accidental vulnerabilities. We use automated static analysis tools that alert us to potential security problems in the code, and those checks must pass in order for code to get deployed.

We have automated tools that monitor for security vulnerabilities in the third-party code dependencies and automatically propose patch updates.

We rely on AWS's mature vulnerability management practice for patching known vulnerabilities at the operating system, virtualization, and hardware layers.

We divide our systems into separate environments for development, staging and production. Each environment is an independent domain with respect to network access control, service

account credentials, and secrets. No access to the production, staging or development environments is allowed except on known protocols and ports via our front-end load balancers.

All access to our services from user devices, or between our client software and our service is protected by TLS version 1.2 or higher.

Our public endpoints, (for example, nametag.co) receive an A+ rating from Qualys SSL Labs.

Authorizing access

To minimize the risk of data exposure, Nametag adheres to the principle of least privilege. Employees are only authorized to access data that they reasonably must handle in order to do their job: all engineers have access to their development environments, fewer engineers have access to the staging environment (only those who need access to perform their jobs), and far fewer have access to the production environment.

All internal systems require our employees to authenticate with unique user accounts.

Data Residency

All Customer Data is maintained in the State of Ohio, United States (for North America and South America Customer Data) or Ireland or Germany (for European Customer Data).

Employee Training

All employees complete mandatory security awareness training once per year. In addition to general resistance to online threats, we teach our staff to resist social engineering attacks through our support channels. All employees are trained in protecting the identities and confidential information of our clients. Although we do not generally handle protected health information (PHI), all employees are trained to identify and report any incidental contact with it.

Authentication

All access to internal systems, including production and business systems, requires hardware backed multi-factor authentication,

Logging

We collect logs from all our servers. We routinely examine logs for suspicious activity and operational issues. We scrub logs of personal data and operational secrets before archiving them.

Business Continuity

All data that we store for you are regularly backed up. We regularly simulate the backup and recovery process to make sure it works smoothly. Copies of backups are stored in multiple data centers in different regions and are encrypted in transit and at rest.

Nametag is insured for cybercrime damage and loss.

To improve public health and the safety and longevity of our team, all Nametag employees who can safely receive vaccines must be vaccinated against COVID-19.

APPENDIX 3: SUB-PROCESSORS

Operational Sub-processors

Operational Sub-processors provide services that are critical to Nametag's services and may process personal information (PI).

Vendor	Purpose	PI
Apollo	Marketing email	No
Apple	iOS App distribution	No
Amazon	Service hosting	Yes
Bugsnag	Performance monitoring for mobile apps	No
Fly	Service hosting	Yes
Google	Service hosting (non-PII) and Android App distribution	No
Honeycomb	Service logging and analytics	No
Postmark	Sending transactional emails	No
Sendgrid	Sending marketing emails	No
Twilio	Sending transactional SMS messages	No

Non-operational sub-processors

Non-operational sub-processors provide services that assist Nametag but are not critical to Nametag's services; non-operational sub-processors do not process any personal information.

Vendor	Purpose
Apple	Mobile device management
Calendly	External scheduling
Figma	Design
Freshworks	Customer relationship management
Google	Email, calendar, documents
GitHub	Source code hosting and continuous integration
GoDaddy	DNS registration
Gusto	Payroll and benefits

HelloSign	**Online document signing**
Microsoft	**Email, calendar, documents**
Pully	**Capitalization table management**
Quickbooks	**Bookkeeping and finance**
Ramp	**Expense reporting and employee credit cards**
Slack	**Internal and partner shared communications**
Webflow	**Marketing website**