DATA PROTECTION AGREEMENT

This Data Protection Agreement ("DPA") supplements any existing and currently valid Beyond Identity Quote, Software as a Service Agreement, or other similar agreement (each "Agreement") previously made between Beyond Identity and the Customer (defined below) (collectively, the "Parties"), if and to the extent: (i) this DPA is required under Applicable Laws (defined below), and (ii) where Beyond Identity Processes Customer Personal Data (both defined below). This DPA supersedes and replaces any prior Data Protection Agreement, or any other prior understanding or agreement, related to the processing of Customer Personal Data in connection with the Agreement. For avoidance of doubt, signature or other acceptance of the Agreement shall be deemed to constitute signature and acceptance of the DPA and the Standard Contractual Clauses incorporated herein including their Exhibits.

1. Definitions

1.1 Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect. Cognate terms shall be construed to have the same meaning.

1.1.1 "**Applicable Laws**" means any laws that regulate the Processing, privacy or security of Customer Personal Data and that are directly applicable to each respective party to this DPA in the context of Beyond Identity Processing Customer Personal Data;

1.1.2 "**Beyond Identity Affiliate**" means an entity belonging to the Beyond Identity group of companies named in Exhibit E as a Beyond Identity Affiliated Subprocessor. The term "Beyond Identity" is inclusive of the applicable Beyond Identity Affiliate when: (i) Applicable Laws require a direct relationship between Beyond Identity Affiliate and the Customer with respect to data protection agreements, and (ii) the Beyond Identity Affiliate processes Customer Personal Data. Beyond Identity represents that it is duly and effectively authorized (or will be subsequently ratified) to act on the Beyond Identity Affiliate's behalf;

1.1.3 "**Customer**" means (i) the person or entity that is indicated below in the signature block, or (ii) if there is no signature block or it is not completed, then Customer is the person or entity that has entered into the Agreement with Beyond Identity. Customer also means a

Customer Affiliate when: (i) Applicable Laws require a direct relationship between Beyond Identity and the Customer's Affiliate with respect to data protection agreements, (ii) Customer is duly and effectively authorized (or subsequently ratified) to act on its Affiliate's behalf, and (iii) Beyond Identity processes the Affiliate's Customer Personal Data;

1.1.4 "**Customer Personal Data**" means any Personal Data Processed by Beyond Identity or a Subprocessor on behalf of the Customer in the provision of the Software;

1.1.5 "**GDPR**" means the General Data Protection Regulation 2016/679 ("GDPR") and any local laws implementing or supplementing the GDPR;

1.1.6 "**Onward Transfer**" means any transfer of Customer Personal Data from Beyond Identity to a Subprocessor;

1.1.7 "**Restricted Transfer**" means any export of Customer Personal Data by Customer to Beyond Identity from its country of origin, either directly or via onward transfer, to a third country in the course of Beyond Identity's provision of the Software under the Agreement that is prohibited under Applicable Laws, unless (a) the destination has been recognized as providing an adequate level of data protection by competent data protection authority, or otherwise in a legally binding way, or (b) Beyond Identity has adopted an appropriate, under Applicable Laws recognized, adequacy mechanism ensuring an adequate level of data protection;

1.1.8 **"Standard Contractual Clauses"** means the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR as to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and incorporated herein by reference; and

1.1.9 "**Subprocessor**" means any contracted service provider (including any third party and Beyond Identity Affiliate but excluding an employee of Beyond Identity or Beyond Identity sub- contractors unless specified in an applicable Statement of Work) Processing Customer Personal Data in the course of Beyond Identity's provisioning of the Software set forth in the Agreement.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", **"Processor",** "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR.

1.3 The word "**include**" shall be construed to mean include without limitation.

2. Processing of Customer Personal Data

2.1 The Parties acknowledge and agree that with regard to the Processing of Customer Personal Data, Customer determines the purposes and means of the Processing of Customer Personal Data, and Beyond Identity processes Customer Personal Data on Customer's behalf in providing the Software.

2.2 Beyond Identity shall:

2.2.1 Process Customer Personal Data only on relevant Customer's documented instructions, as set out in the Agreement, this DPA, including Customer providing instructions via configuration tools and APIs made available by Beyond Identity with the Software, and as required by Applicable Laws (the "**Documented Instructions**"). Any additional or alternate instructions, having an impact to the Software must be agreed upon by the Parties separately in writing; and

2.2.2 Unless prohibited by Applicable Law, Beyond Identity shall inform the Customer in advance if Beyond Identity determines that: (i) Customer's instructions conflict with Applicable Laws; or
(ii) Applicable Laws require any processing contrary to the Customer's instructions.

2.3 Customer shall:

2.3.1 Be responsible for complying with Applicable Laws when making decisions and issuing instructions for the Processing of Customer Personal Data, including securing all permissions, consents or authorizations that may be required.

2.3.2 Defend and indemnify Beyond Identity, Beyond Identity Affiliates, and Beyond Identity Subprocessors for any claim brought against them arising from an allegation of Customer's breach of this section, whether by a Data Subject or a government authority. This provision does not diminish Customer or Data Subject's rights under Applicable Laws related to Beyond Identity's adherence to its obligations under Applicable Laws. In the event of such a claim, the Parties shall follow the process set forth in the Agreement and if none, then Beyond Identity will: (a) notify Customer of such claim, (b) permit Customer to control the defense or settlement of such claim; provided, however, Customer shall not settle any claim in a manner that requires Beyond Identity to admit liability without Beyond Identity's prior written consent, and (c) provide Customer with reasonable assistance in connection with the defense or settlement of such claim, at Customer's cost and expense. In addition, Beyond Identity may participate in defense of any claim, and if Customer is already defending such claim, Beyond Identity's participation will be at Beyond Identity's expense.

3. Beyond Identity Personnel

Beyond Identity shall take reasonable steps to:

3.1 Implement appropriate security controls designed to ensure access to Customer Personal Data is strictly limited to those individuals who need to know/access the relevant Customer Personal Data as reasonably necessary for the purposes outlined in this DPA, the Agreement or required under Applicable Laws; and

3.2 Ensure all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Beyond Identity shall in relation to the Processing of Customer Personal Data maintain appropriate technical and organizational measures as specified in the Agreement and designed to ensure a level of security appropriate to the risk, including, as appropriate, the measures referred to in Applicable Laws.

4.2 In assessing the appropriate level of security, Beyond Identity shall take into account the nature of the data and the Processing activities in assessing the risks posed by a potential Personal Data Breach.

5. Subprocessing

5.1 To the extent required under Applicable Laws, Customer authorizes Beyond Identity to appoint (and permit each Subprocessor appointed in accordance with this section to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Agreement.

5.2 Beyond Identity may continue to use those Subprocessors already engaged as of the date of this DPA specified in Exhibit E, subject to Beyond Identity in each case meeting the obligations set out in section 5.5.

5.3 Customer agrees to Beyond Identity maintaining and updating its list of Subprocessors as outlined in Exhibit E.

5.4 Beyond Identity shall provide notice of a proposed new Subprocessor to the Customer, at least 30 days prior to Beyond Identity's use of the new Subprocessor to Process Customer Personal Data, through the applicable Software, where Customer may elect to subscribe to such notices. Customers may sign up for email Subprocessor notifications by submitting a request to legal@beyondidentity.com. During the notice period, Customer may object to a change in Subprocessor in writing and Beyond Identity may, in its sole discretion, attempt to resolve Customer's objection, including providing the Software without use of the proposed Subprocessor. If (a) Beyond Identity provides Customer written notice that it will not pursue an alternative, or (b) such an alternative cannot be made available by Beyond Identity to Customer within 90 days of Customer providing notice of its objection, then in either case, and notwithstanding anything to the contrary in the Agreement or order, Customer may terminate the Agreement or order to the extent that it relates to the Software which require the use of the proposed Subprocessor.

5.5 With respect to each Subprocessor, to the extent required under Applicable Laws, Beyond Identity shall:

5.5.1 Before the Subprocessor first Processes Customer Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by Applicable Laws, this DPA and the Agreement;

5.5.2 Ensure that the arrangement between Beyond Identity and Subprocessor is governed by a written contract which offers substantially the same level of protection for Customer

Personal Data as required by this DPA and Applicable Laws, including Customer's ability to protect the rights of Data Subjects in the event Beyond Identity is insolvent, liquidated or otherwise ceases to exist;

5.5.3 Apply an adequacy mechanism recognized by Customer's Supervisory Authority as ensuring an adequate level of data protection under Applicable Laws where Subprocessor's Processing of Customer Personal Data involves a Restricted Transfer;

5.5.4 Maintain copies of the agreements with Subprocessors as Customer may request from time to time. To the extent necessary to protect Confidential Information, Beyond Identity may redact the copies prior to sharing with Customer; and

5.5.5 Notify Customer of Subprocessor's relevant failure to comply with obligations set out by Applicable Laws and this DPA where Beyond Identity has received notice of such.

6. Data Subject Rights

6.1 Customer represents and warrants to provide appropriate transparency to any Data Subjects concerned of Beyond Identity's Processing of Customer Personal Data and respond to any request filed by Data Subjects as required under Applicable Laws.

6.2 Taking into account the nature of the Customer Personal Data Processing, Beyond Identity shall:

6.2.1 Not respond to the Data Subject request itself or by Subprocessor unless required by Applicable Laws; and

6.2.2 Notify Customer without undue delay if Beyond Identity or any Subprocessor receives a request from a Data Subject under any Applicable Laws in respect to Customer Personal Data; and

6.2.3 Reasonably assist Customer through appropriate technical and organizational measures to fulfill Customer's obligation to respond to Data Subject requests arising under Applicable Law, and where Customer is unable to respond to Data Subject requests through the information available by the Software.

7. Personal Data Breach

8.1 Upon Beyond Identity becoming aware of any Personal Data Breach affecting Customer Personal Data, Beyond Identity shall without undue delay, and within the timeframes required by Applicable Laws, notify Customer of such Personal Data Breach. To the extent known, Beyond Identity shall provide Customer with sufficient information to meet obligations under Applicable Laws to report or inform Data Subjects of such Personal Data Breach.

7.2 Beyond Identity shall cooperate with Customer and take commercially reasonable steps to assist in the investigation, mitigation, and remediation of such Personal Data Breach.

8. Obligations to Assist Customer

Taking into account the nature of the Processing and information available to Customer in each case solely in relation to Beyond Identity's Processing of Customer Personal Data, Beyond Identity shall provide reasonable assistance to Customer with any:

8.1 Necessary data protection impact assessments required of Customer by Applicable Laws;

8.2 Consultation with or requests of a competent data protection authority;

8.3 Inquiries about Beyond Identity's Processing of Customer Personal Data pursuant to the Agreement and this DPA.

9. Deletion of Customer Personal Data

9.1 Processing of Customer Personal Data by Beyond Identity shall only take place for the duration specified in Exhibit A.

9.2 At the end of the duration specified in Exhibit A or upon termination of the Software and pursuant to the Agreement:

9.2.1 Customer Personal Data will be deleted within 90 days of the Software being deprovisioned unless the retention of Customer Personal Data is required under Applicable Laws.

9.2.2 Upon Customer's written request, Beyond Identity shall:

9.2.2.1 Make Customer Personal Data available for return to Customer where such a request has been made prior to deletion by reasonably providing Customer with a means to retrieve Customer Personal Data from the Software; and

9.2.2.2 Provide a written certification of deletion of Customer Personal Data to Customer.

10. Audit Rights

10.1 Subject to sections 10.2 to 10.4, Beyond Identity shall make available to Customer on request information necessary to demonstrate compliance with Applicable Laws and this DPA.

10.2 To the extent required by Applicable Laws, Beyond Identity shall contribute to audits by Customer or an independent auditor engaged by the Customer, that is not a competitor of Beyond Identity, in relation to the Processing of the Customer Personal Data.

10.3 Information and audit rights of the Customer only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Applicable Laws.

10.4 Notwithstanding the foregoing, Beyond Identity may exclude information and documentation that would reveal the identity of other Beyond Identity customers or information that Beyond Identity is required to keep confidential. Any information or records provided pursuant to this assessment process shall be considered Beyond Identity's Confidential Information and subject to the Confidentiality section of the Agreement.

11. Restricted Transfers from jurisdictions requiring safeguards to cross-border data transfer

11.1 Where, in the use of the Software or performance of the Agreement, Customer directly, indirectly or via onward transfer makes a Restricted Transfer of Customer Personal Data originating from the EEA, Israel, Switzerland and/or the United Kingdom ("UK") to a third country, not determined by the European Commission, on the basis of Article 45 of the GDPR, or another competent supervisory authority under Applicable Laws, offering an adequate level of data protection, and where Beyond Identity has not adopted another legally sufficient adequacy mechanism and provided notice to the Customer, the Standard Contractual Clauses will be incorporated into this DPA and shall apply as follows:

11.1.1 The Parties acknowledge and agree:

11.1.1.1 Beyond Identity will be a Data Importer acting as Processor of Customer Personal Data (or Subprocessor, as the context below requires) to a Restricted Transfer.

11.1.1.2 Where Customer will be a Data Exporter acting as Controller, Module 2 (Controller to Processor) will apply to a Restricted Transfer.

11.1.1.3 Where Customer will be a Data Exporter acting as a Processor, Module 3 (Processor to Processor) will apply to a Restricted Transfer. Taking into account the nature of the Processing, Customer agrees that it is unlikely that Beyond Identity will know the identity of Customer's Controllers because Beyond Identity has no direct relationship with Customer's Controllers and therefore, Customer will fulfill Beyond Identity's obligations to Customer's Controllers under the Module 3 (Processor to Processor) Clauses.

11.1.1.4 Where Beyond Identity will be Data Importer Processing Customer Personal Data in its own discretion as Controller in the provisioning of the Software agreed, e.g., for administering the Agreement, Module 1 (Controller to Controller) will apply to the relationship between Customer (Data Exporter) and Beyond Identity (Data Importer).

11.1.2 Clause 8.1 (Instructions). The Parties acknowledge that Customer's instructions may not conflict with the Software. Any additional or alternate instructions, having impact to the Software, must be agreed upon separately between the Parties. The following is a mutually agreed instruction: (a) Processing of Customer Personal Data in accordance with the Agreement and any applicable orders; (b) Processing initiated by users in their use of the Beyond Identity Softwares, and (c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

11.1.3 Clause 8.5 (Duration of processing and erasure or return of data). Customer acknowledges and expressly agrees that the process described in Section 9 of the DPA shall govern the fulfillment of requirements related to data erasure and return of Customer Personal Data.

11.1.4 Clause 8.9(c, d) (Audit). The Parties agree the audits described in Clause 8.9(c, d) shall be carried out in accordance with Section 10 of this DPA. To the extent Clause 8.9(c, d) additionally requires Beyond Identity's facilities be submitted for inspection, Customer may contact Beyond Identity through prior written notice to request an on-site audit of the procedures relevant to the protection of Customer Personal Data. Customer shall reimburse Beyond Identity for any time expended for any such on-site audit at Beyond Identity's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Beyond Identity shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. Customer shall promptly notify Beyond Identity with information regarding any non-compliance discovered during the course of an audit. In order to align efforts and to keep actions consistent, Customer shall be the relevant body carrying out audits towards Beyond Identity for itself and Controllers, where Customer acts as a Processor under the instruction of a Controller Beyond Identity has no direct relationship with.

11.1.5 Clause 9 (Use of sub-processors). The Parties agree to and choose Option 2 (General written authorization) and specify the time period set forth in Section 5 of this DPA while Customer further acknowledges and agrees that Beyond Identity may engage existing Subprocessors (Exhibit E), and new Subprocessors as described there. Where Customer is a Processor to Customer Personal Data, Customer agrees and warrants to be duly authorized to receive and pass on information about Beyond Identity's new Subprocessor engagement to Controllers with whom Beyond Identity has no direct relationship, assisting Beyond Identity to meet its obligation under Clause 9 towards the Controllers. Customer acknowledges that Beyond Identity maintains an up-to-date *List of Subprocessors* online as outlined in Exhibit E.

11.1.6 Clause 11(a) (Redress). The Parties agree that the option provided shall not apply.

11.1.7 Clause 13 (Supervision). The options in Clause 13 will be selected in line with the Customer's establishment.

11.1.8 Clause 17 (Governing law). The Parties agree to and choose Option 2; where such law does not allow for third-party beneficiary rights, the Parties agree that this shall be the law of the Netherlands.

11.1.9 The Exhibits A to E of this DPA substitutes the Annexes I to III required under the Standard Contractual Clauses providing the mandatory information under Applicable Laws.

11.1.10 Where the Restricted Transfer concerns Customer Personal Data originating from Switzerland, in line with the Swiss Federal Data Protection and Information Commissioner's statement as of August, 27, 2021, the following additional requirements shall apply to the extent the Customer Personal Data transferred is exclusively subject to the Swiss Data Protection Act (FADP) or to both the FADP and the GDPR: (i) The term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in

accordance with Clause 18 (c) of these Standard Contractual Clauses. (ii) Insofar as the data

transfers underlying these Standard Contractual Clauses are exclusively subject to the FADP, references to the GDPR are to be understood as references to the FADP. Insofar as the data transfers underlying these Standard Contractual Clauses are subject to both the FADP and the GDPR, the references to the GDPR are to be understood as references to the FADP insofar as the data transfers are subject to the FADP. (iii) Until the revised Swiss Data Protection Act (rev. FADP) enters into force, the provisions of these Standard Contractual Clauses and all Exhibits also protect any Customer Personal Data to the extent that these provisions are applicable to them under Applicable Swiss Laws.

11.1.11 Where the Restricted Transfer concerns Customer Personal Data originating from the UK, the Standard Contractual Clauses will apply subject to the conditions set out by the United Kingdom Information Commissioner Office's ("ICO") International Data Transfer Addendum to the Standard Contractual Clauses that shall be incorporated herein by reference. The Parties acknowledge and agree that this DPA and the Exhibits A to E (i) provide the information needed and required by the ICO for completing Part One of the International Data Transfer Addendum, and (ii) shall be governed by the laws and courts of England and Wales (Clauses 17 and 18 of the Standard Contractual Clauses) for completing Part Two of the International Data Transfer Addendum.

11.2 Where the Restricted Transfer concerns Customer Personal Data originating from Argentina, the standard contractual clauses made under Regulation No. 60-E/2016 will be incorporated into this DPA by reference and shall apply to the extent required under Applicable Laws and where this DPA does not provide adequate safeguards.

11.3 Where the Restricted Transfer concerns Customer Personal Data originating from another jurisdiction requiring certain privacy safeguards, standard contractual clauses, or any other contractual privacy provisions, not provided through this DPA, the Standard Contractual Clauses will be incorporated into this DPA by reference and shall apply to the extent required under Applicable Laws and where this DPA does not provide adequate safeguards. For the avoidance of any doubt, by applying the Standard Contractual Clauses in this event, the Parties do not intend to grant third-party beneficiary rights to Data Subjects under the Standard Contractual Clauses when Data Subjects concerned would not otherwise benefit from such rights under the Applicable Laws or this DPA.

12. General Terms

Governing law and jurisdiction

12.1 The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity. Where, in line with section 11 of this DPA the Standard Contractual Clauses apply, and it is required under Applicable Laws, for disputes arising the governing law and jurisdiction are stipulated in Clause 17 of the Standard Contractual Clauses.

Order of precedence

12.2 Any conflict between the terms of the Agreement and this DPA related to the processing of Customer Personal Data are resolved in the following order of priority: (1) the Standard Contractual Clauses (where applicable and materially affecting the adequacy of the Restricted Transfer); (2) this DPA; (3) the Agreement. For the avoidance of doubt, provisions in this DPA, that merely go beyond the Standard Contractual Clauses without contradicting them, shall remain valid. The same applies to conflicts between this DPA and the Agreement where this DPA shall only prevail regarding the Parties' Personal Data protection obligations.

12.3 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, should this not be possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. The foregoing shall also apply if this DPA contains any omission.

12.4 Notwithstanding sections 12.2 and 12.3, the terms of the Agreement shall remain in full force and effect.

12.5 For the avoidance of doubt, by applying the provisions of this DPA, the Parties do not intend to grant third-party beneficiary rights to Data Subjects under the DPA when those Data Subjects would not otherwise benefit from such rights under the Applicable Laws.

Limitation of Liability

12.6 Unless required by Applicable Laws, Customer shall exercise any right or seek any remedy on behalf of itself, its Affiliates, and any other Controller that Customer instructs Beyond Identity to process Customer Personal Data for under this DPA (collectively, the "Customer Parties"). Customer shall exercise any such rights or seek any such remedies in a combined manner for all Customer Parties together, rather than separately for each entity individually. To the maximum extent allowed by Applicable Laws, the limitations of liability and any exclusions of damages set forth in the Agreement govern the aggregate liability for all Customer Parties' claims arising out of or related to this DPA, and/or the Agreement against Beyond Identity and any Beyond Identity Affiliate(s). These limitations of liability and exclusions of damages apply to all claims, whether arising under contract, tort or any other theory of liability, and any reference to the liability of Beyond Identity means the aggregate liability of Beyond Identity and all Beyond Identity Affiliates together for claims by Customer and all other Customer Parties.

12.7 To the extent required by Applicable Laws, (i) this section is not intended to modify or limit the Parties' liability for Data Subject claims made against a Party where there is joint and several liability, or (ii) limit either Party's responsibility to pay penalties imposed on such Party by a regulatory authority.

The Parties by their duly authorized representatives have accepted this DPA to be effective as of the Effective Date of the Agreement.

BEYOND IDENTITY

EXHIBIT A

DESCRIPTION OF PROCESSING AND TRANSFER OF CUSTOMER PERSONAL DATA

This Exhibit A includes certain details of the Processing and Restricted Transfer of Customer Personal Data as required by Article 28(3) GDPR and the Standard Contractual Clauses.

Subject matter, nature and duration of the Processing / transfer of Customer Personal Data

The subject matter, nature and duration of the Processing and the transfer of the Customer Personal Data are set out in the Agreement and this DPA, and depend on the nature and scope of the Software, manner of receipt, collection, storage, use, dissemination (towards Subprocessors in line with the Agreement and this DPA), retention and erasure of Customer Personal Data, and Customer's Documented Instructions.

Purpose for which the Personal Data is Processed / transferred on behalf of the Customer

The purposes of the Processing and transfer of the Customer Personal Data is to enable Beyond Identity and Beyond Identity's Subprocessor to provision and deliver the Software and perform its obligations as set forth in the Agreement, this DPA, and Customer's Documented Instructions or as otherwise agreed by the Parties in mutually executed written form.

Categories of Personal Data Processed / Transferred including sensitive Personal Data

The Customer, rather than Beyond Identity, determines which categories of Personal Data exist and will be disclosed to and Processed by Beyond Identity in the provisioning of the Software because (i) Customer's infrastructure (e.g., endpoint, virtual machine and cloud environments) is unique in configurations and naming conventions, (ii) Beyond Identity enables the Customer to configure settings in the Software, and (iii) Customer controls (such as via deployment, configuration, and submission) which Customer Content is uploaded, or is collected by, the Software.

Categories of Data Subjects whose Personal Data is Processed

The Customer, rather than Beyond Identity, determines which Data Subjects' Personal Data is Processed by Beyond Identity through the Customer Content put into, or collected by, the Software.

Frequency of the Transfer of Personal Data

Taking into account Beyond Identity's Customer Personal Data Processing including the manner of receipt, collection, storage, and use of Customer Personal Data, the frequency of the transfer of Customer Personal Data depends on the nature and scope of the Software agreed to under the Agreement, the Customer's Documented Instructions and Beyond Identity's need to transfer Personal Data for the performance of the Services. Consequently, transfers may happen on either a continuous or one-off basis, until the termination of the Agreement.

Period for which the Personal Data will be Retained, or Criteria Used to Determine that Period

As set out in the Agreement, this DPA and Customer's Documented Instructions.

Subject Matter, Nature and Duration of the Processing with respect to Transfers to Subprocessors

Beyond Identity maintains an up-to-date list of Subprocessors including name, contact details, processing and address, and such list is available for registered users upon request by submitting a request to legal@beyondidentity.com.

The Duration of the Processing of Customer Personal Data with respect to transfers to Subprocessors is consistent with the Agreement and this DPA.

EXHIBIT B

LIST OF PARTIES

Data exporter:

Name: Customer

Address: As specified in the Agreement

Contact person's name, position and contact details: As specified in the signature box of this DPA

Activities relevant to the data transferred under these Clauses: As specified in Exhibit A

Role: Controller and/or, to the extent applicable, Processor

Data importer:

Name: Beyond Identity Inc.

Address: As specified in the Agreement

Contact person's name, position and contact details: General Counsel, legal@beyondidentity.com

Activities relevant to the data transferred under these Clauses: As detailed in Exhibit A to this DPA and the Agreement

Role: Processor and/or, to the extent applicable, Controller

EXHIBIT C

COMPETENT SUPERVISORY AUTHORITY

Where Customer makes a Restricted Transfer of Customer Personal Data originating from the EEA, the competent supervisory authority shall be determined in accordance with Clause 13 of the Standard Contractual Clauses.

Where Customer makes a Restricted Transfer of Customer Personal Data originating from Switzerland, and the Standard Contractual Clauses apply, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner with respect to the Customer Personal Data originating from Switzerland.

Where Customer makes a Restricted Transfer of Customer Personal Data originating from the UK, and the Standard Contractual Clauses apply, the competent supervisory authority shall be the ICO with respect to the Customer Personal Data originating from the UK.

Where Customer makes a Restricted Transfer of Customer Personal Data originating from another jurisdiction requiring the determination of the competent supervisory authority under Applicable Laws, the competent supervisory authority shall be determined by Applicable Laws.

BEYOND IDENTITY

EXHIBIT D

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Security Control Category	Description
1. Governance	a. Assign to an individual or a group of individuals appropriate roles for developing, coordinating, implementing, and managing Beyond Identity's administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Personal Data b. Use of data security personnel that are sufficiently trained, qualified, and experienced to be able to fulfill their information security-related functions
2. Risk Assessment	a. Conduct periodic risk assessments designed to analyze existing information security risks, identify potential new risks, and evaluate the effectiveness of existing security controls b. Maintain risk assessment processes designed to evaluate likelihood of risk occurrence and material potential impacts if risks occur c. Document formal risk assessments d. Review formal risk assessments by appropriate managerial personnel
3. Information Security Policies	a. Create information security policies, approved by management, published and communicated to all employees and relevant external parties. b. Review policies at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
4. Human Resources Security	a. Maintain policies requiring reasonable background checks of any new employees who will have access to Personal Data or relevant Beyond Identity Systems, subject to local law b. Regularly and periodically train personnel on information security controls and policies that are relevant to their business responsibilities and based on their roles within the organization
5. Asset Management	a. Maintain policies establishing data classification based on data criticality and sensitivity b. Maintain policies establishing data retention and secure destruction requirements c. Implement procedures to clearly identify assets and assign ownership

6. Access Controls	a. Identify personnel or classes of personnel whose business functions and responsibilities require access to Personal Data, relevant Beyond Identity Systems and the organization's premises b. Maintain controls designed to limit access to Personal Data, relevant Beyond Identity Systems and the facilities hosting the Beyond Identity Systems to authorized personnel c. Review personnel access rights on a regular and periodic basis d. Maintain physical access controls to facilities containing Beyond Identity Systems, including by using access cards or fobs issued to Beyond Identity personnel as appropriate e. Maintain policies requiring termination of physical and electronic access to Personal Data and Beyond Identity Systems after termination of an employee f. Implement access controls designed to authenticate users and limit access to Beyond Identity Systems g. Implement policies restricting access to the data center facilities hosting Beyond Identity Systems to approved data center personnel and limited and approved Beyond Identity personnel h. Maintain dual layer access authentication processes for Beyond Identity employees with administrative access rights to Beyond Identity Systems
7. Cryptography	a. Implement encryption key management procedures b. Encrypt sensitive data using a minimum of AES/128 bit ciphers in transit and at rest
8. Physical Security	a. Require two factor controls to access office premises b. Register and escort visitors on premises
9. Operations Security	a. Perform periodic network and application vulnerability testing using dedicated qualified internal resources b. Contract with qualified independent 3rd parties to perform periodic network and application penetration testing c. Implement procedures to document and remediate vulnerabilities discovered during vulnerability and penetration tests
10. Communications Security	a. Maintain a secure boundary (e.g. using firewalls and network traffic filtering) b. Require internal segmentation to isolate critical systems from general purpose networks c. Require periodic reviews and testing of network controls
11. System Acquisition, Development and Maintenance	a. Assign responsibility for system security, system changes and maintenance b. Test, evaluate and authorize major system components prior to implementation
12. Supplier Relationships	Periodically review available security assessment reports of vendors hosting the Beyond Identity Systems to assess their security controls and analyze any exceptions set forth in such reports

13. Information Security Breach Management	a. Monitor the access, availability, capacity and performance of the Beyond Identity Systems, and related system logs and network traffic using various monitoring software and services b. Maintain incident response procedures for identifying, reporting, and acting on Security Breaches c. Perform incident response table-top exercises with executives and representatives from across various business units d. Implement plan to address gaps discovered during exercises e. Establish a cross-disciplinary Security Breach response team
14. Business Continuity Management	a. Design business continuity with goal of 99.9% uptime SLA b. Conduct scenario based testing annually
15. Compliance	a. Establish procedures designed to ensure all applicable statutory, regulatory and contractual requirements are adhered to

Exhibit E

LIST OF SUBPROCESSORS

Beyond Identity maintains an up-to-date list of Subprocessors available for registered users upon request by submitting a request to legal@beyondidentity.com.