(Global) Data Processing Addendum

This Data Protection Addendum ("**DPA**") is hereby incorporated into the agreement that references this DPA between the ForgeRock entity identified on the applicable Order Form ("**ForgeRock**") and the customer identified on such Order Form ("**Customer**") and that governs Customer's access to ForgeRock's software and/or services ("**Agreement**"). Any capitalised terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

In consideration of the mutual covenants and promises contained herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions: For the purpose of this DPA:

1.1 "**Data Protection Laws**" means any applicable law or regulation concerning data protection and/or privacy that governs the processing of personal data including but not limited to the following laws and any supervisory guidance published in respect thereto: (i) General Data Protection Regulation (EU) 2016/679 ("**GDPR**") (ii) Privacy Act 1988 (Australia), (iii) Personal Information Protection and Electronic Documents Act [SC 2000 c.5] (Canada) (iv) Personal Information Protection Act, [SA 2003 c P-6.5] (Alberta), (v) Personal Information Protection Act [SBC 2003 c.63] (British Columbia) (vi) Act respecting the protection of personal information in the private sector (CQLR c P-39.1) (Quebec) (vii) Personal Data Protection Act 2012 (Singapore) (viii) Federal Act on Data Protection of 19 June 1992, as revised (Switzerland) (ix) Virginia Consumer Data Protection Act, (x) Colorado Privacy Act (xi) Connecticut Data Privacy Act, (xii) Utah Consumer Privacy Act (xiii) California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 and (xiv) the UK Data Protection Act 2018 and the GDPR as each is amended in accordance with the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended by SI 2020 no. 1586) and incorporated into UK law under the UK European Union (Withdrawal) Act 2018.

1.2 "**EEA**" means the European Economic Area plus Switzerland.

1.3 "**processing**", "**data subject**", "**controller**", and "**processor**" and "**special categories of personal data**" shall all have the meanings given to them by GDPR or applicable data protection laws to which the Customer PII may be subject to the extent that such concepts exist in such laws;

1.4 "**Data Subject Request**" means a request made to the Customer by a data subject under Applicable Data Protection Law, in relation to the data subject's privacy law rights, including but not limited to obtaining a copy of Customer PII.

1.5 "**Third Party Request**" means any request, correspondence, inquiry, or complaint from a regulatory authority or other competent governmental organisation;

2. Customer's Acknowledgement:

2.1 Customer acknowledges that ForgeRock, its Affiliates and its sub-processors may come into possession of Customer PII in connection with the provision of ForgeRock's generally available hosted, on demand, web-based services or in connection with ForgeRock's support of ForgeRock's self-service (on-premise) software ("**Services**");

2.2 Customer and ForgeRock agree that with regard to the processing of Customer PII, Customer may act either as a controller or processor and ForgeRock is a processor. ForgeRock shall only process Customer PII as set forth in Clause 3 below.

2.3 Customer acknowledges that ForgeRock's Chief Privacy Counsel is the designated point of contact in relation to ForgeRock's processing of Customer PII. Contact details: privacy@forgerock.com.

3. ForgeRock Obligations When Acting As A Processor: ForgeRock agrees:

3.1 that it will only process Customer PII for the performance of the Services in accordance with the Customer's instructions which are set out in this DPA, or as otherwise mutually agreed between the parties in writing, and that it will notify the Customer if ForgeRock considers any such processing of Customer PII to be in violation of any Data Protection Laws applicable to ForgeRock. Specific details of the processing are set out in Schedule 1 (Processing Activities[1]) of this DPA;

3.2 that if it is legally required to process Customer PII otherwise than as instructed by Customer, it will notify Customer before such processing occurs unless prohibited from doing so by law;

[1] Further details of ForgeRock's processing activities are available at ForgeRock's Privacy Hub: https://www.forgerock.com/privacy-hub

3.3 to provide Customer with a number of self-service features via the Services, including the ability to delete, obtain a copy of, or restrict use of Customer PII. Customer acknowledges and agrees that it will access the self-service features via the following link:

https://backstage.forgerock.com/knowledge/backstagehelp/article/a64008367#ScvlBS [2].

Customer may use such self-service features to assist in complying with its obligations under Applicable Data Protection Law with respect to responding to Data Subject Requests via the Services at no additional cost. Upon the Customer's request, ForgeRock will provide reasonable, additional and timely assistance to Customer in complying with Data Subject Requests to the extent Customer does not have the ability to resolve a Data Subject Request through self-service features made available via the Services;

3.4 to ensure that its personnel who have access to Customer PII are bound by, and made aware of, their obligations of confidentiality with respect to protecting Customer PII;

3.5 taking into account the state of the art and the costs of implementation, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to Customer PII or data subjects, which shall include protecting Customer PII against accidental or unlawful destruction, loss, alteration, or unauthorised disclosure or access ("**Customer PII Breach**"). Specific details of the technical and organisational measures applicable to the processing are set out in Schedule 2 (Technical and Organisational Security Measures) of this DPA;

3.6 without undue delay after becoming aware of a Customer PII Breach, to notify Customer of a Customer PII Breach. Such notification shall include, taking into account the nature of the processing and the information available to ForgeRock, any information relevant to assist the Customer with its own notification obligations under applicable law, including:

(a) a description of the nature of the Customer PII including where possible, the categories and approximate number of affected individuals;

(b) a description of the categories and approximate number of Customer PII records concerned;

(c) the name and contact details of the Chief Privacy Counsel or other contact point where more information can be obtained;

(d) a description of the likely consequences of the Customer PII Breach;

(e) a description of the measures taken or proposed to be taken to address the Customer PII Breach, including, where appropriate, measures to mitigate its possible adverse effects; and

(f) where, and in so far as, it is not possible to provide the information according to provision immediately above at the same time, ForgeRock shall provide the information in phases without further undue delay.

4. Customer Audit:

4.1 **Audit Rights**: Customer or its independent third-party auditor may audit ForgeRock's data processing activities relevant to the Customer PII processed under this DPA only if:

(a) ForgeRock has failed to provide sufficient evidence of its compliance with its obligations under this DPA; or

(b) Customer has reasonable grounds to suspect that ForgeRock is not complying with its obligations under this DPA; or

(c) ForgeRock has experienced a Customer PII Breach; or

(d) an audit is formally requested by a data protection authority or other competent governmental organisation; or

(e) mandatory data protection law provides Customer with a direct audit right.

4.2 **Audit Support**: Where Customer audits ForgeRock's environment, ForgeRock will reasonably support the Customer in its audit processes.

4.3 **Audit Restrictions**:

[2] Access to the Customer Advisory sitting behind this link will be made available to Customer during the 'customer onboarding' process.

(a) The Customer audit will be limited (i) in frequency to once in any twelve-month period (ii) in time to a maximum of 3 business days; and (iii) in scope as reasonably agreed in advance between the parties.

(b) Reasonable advance notice of at least ninety days is required, unless Data Protection Laws require otherwise.

(c) ForgeRock and Customer will use current certifications or other current audit reports to minimize repetitive audits.

4.4 The provisions of this sub clause exist without prejudice to any audit rights and obligations set forth elsewhere in this DPA.

5. Sub-Processors:

5.1 **Current sub-processors**: Customer provides a general authorization for ForgeRock to engage onward sub-processors and/or ForgeRock Affiliates notified to Customer. A list of ForgeRock's current sub-processors and/or ForgeRock Affiliates, including, but not limited to, a description of processing activities and processing location, is available on the Privacy Documentation page of ForgeRock's website (link: https://www.forgerock.com/resources/view/125449877/legal-document/privacy-documentation-sub-processor-affiliate-list.pdf).

5.2 **New sub-processors**: Customer acknowledges and agrees that the method by which ForgeRock will inform Customer of new sub-processors and/or ForgeRock Affiliates will be as follows: Customer shall register to receive an email notification of new sub-processors and/or ForgeRock Affiliates via the following link:

https://backstage.forgerock.com/knowledge/backstagehelp/article/a79270396 ("**Sub-Processor Site**")[3]

the notification will set out each sub-processor's name, location and processing activities.

5.3 **Customer's objection right**: If Customer objects to ForgeRock's use of a new sub-processor or ForgeRock Affiliate as notified in accordance with the terms of this clause, Customer shall notify ForgeRock in writing within ten (10) business days after receipt of the information via the Sub-Processor Site. In the event Customer puts forward a reasonable objection to a new sub-processor or ForgeRock Affiliate, ForgeRock agrees to engage in good faith discussions with Customer to address Customer's objection.

5.4 **Subcontracts**: Where ForgeRock subcontracts its data protection obligations in accordance with the terms of this clause, it will do so by way of a written agreement with the sub-processor which imposes the same material obligations on the sub-processor as are imposed on ForgeRock under this DPA and which requires the sub-processor to implement and maintain appropriate technical and organisational measures. ForgeRock will remain liable for any breach of this DPAthat is caused by an act, error, or omission of its sub-processors.

6. International Provisions

6.1 **Cross border data transfers**. To the extent Customer's use of the Services requires:

(a) an 'adequacy' mechanism to lawfully process UK and/or EEA originating Customer PII (via sub-processor(s) and/or a ForgeRock Affiliate) in locations outside of the UK and/or EEA, the relevant EU standard contractual clauses set forth the Privacy Documentation page of ForgeRock's website (link: https://www.forgerock.com/privacydocumentation/eusccs) will apply; and

(b) a sub-processor or ForgeRock Affiliate to process Customer PII in a country where Data Protection Laws may differ from those in the country of origin, then ForgeRock shall bind such sub-processor to terms that are substantively similar to the terms of this DPA.

6.2 **Jurisdiction Specific Terms**. To the extent ForgeRock processes Customer PII originating from and protected by Data Protection Laws in one of the jurisdictions listed in Schedule 3 (Jurisdiction Specific Terms) of this DPA, the terms specified in Schedule 3 with respect to the applicable jurisdiction(s) apply in addition to the terms of this DPA.

6.3 **Change of circumstances**. If ForgeRock's compliance with its international data transfer obligations is affected by circumstances outside of ForgeRock's control, including if a legal instrument for international data transfers is invalidated, amended, or replaced, then the Customer and ForgeRock will work together in good faith to reasonably resolve such non-compliance.

[3] The Sub-Processor Site will be made available to Customer during the 'customer onboarding' process. ForgeRock recommends that Customer registers to the Sub-Processor Site using an appropriate email alias (for example ciso@customerco.com)

7. Change Management

7.1 **The** Customer may elect for ForgeRock to revise and/or update this DPA or any document referenced herein to reflect changes mandated under Data Protection Laws ("**Mandatory Amendments**") by registering to:

https://docs.google.com/forms/d/e/1FAIpQLSeZHN9ZSaiJspTzT2yYX1wyQeNkALPgyhe5k1VOe1jH3pYWSg/viewform?usp=sf_link ("**Updating Service**")[4].

7.2 **Should** Customer exercise its discretion to subscribe to the Updating Service:

(a) ForgeRock shall notify Customers of Mandatory Amendments;

(b) any Mandatory Amendments shall be deemed accepted fifteen (15) days after the Customer receives notification of any changes via the Updating Service, providing the Customer has not provided a reasonable written objection to such Mandatory Amendments within such fifteen (15) day period; and

7.3 **Should** the Customer provide a reasonable written objection under this clause, ForgeRock agrees to engage in good faith discussions with the Customer to resolve such objection and maintain data processing in compliance with Data Protection Laws.

8. Effect of Termination. After termination of the Agreement ForgeRock will cease all processing of Customer PII on behalf of Customer and delete all Customer PII or, if reasonably practicable to do so, return Customer PII, unless ForgeRock is subject to a legal requirement to store Customer PII.

9. Third Party Requests: ForgeRock agrees that, in respect of any Third Party Request received in relation to disclosing Customer PII, it shall:

(a) reject any request for Customer PII that is not legally binding;

(b) where legally permissible and without undue delay (i) notify the Customer of the receipt of the Third Party Request and the particulars associated with such request and (ii) consult the Customer and action Customer's reasonable instructions in relation to making any disclosure of Customer PII;

(c) accept any contractually agreed requests for Customer PII disclosures that are authorised by the Customer.

10. Conflict: Where there is any conflict between the terms of this DPA and any other agreement entered into between the parties pertaining to the subject matter of this DPA, the terms of this DPA shall prevail.

[4] ForgeRock recommends that Customer subscribes to the Updating Service using an appropriate email alias (for example dpo@customerco.com)

SCHEDULE 1: PROCESSING ACTIVITIES

PRELIMINARY

Definitions: additional definitions for the purposes of this Schedule 1:

Customer Contact PII: personal data relating to Customer's relationship with ForgeRock, including the names and/or contact information of individuals authorized by Customer to access Customer's account with ForgeRock including any personal data ForgeRock may need to collect for the purpose of identity verification.

(A) LIST OF PARTIES

(1) Data exporter(s):

Name: the Customer

Address: as specified in the DPA or the Agreement

Activities relevant to the data transferred under these Clauses: the activities specified herein.

Signature and date: n/a

Role (controller/processor): Controller

(2) Data importer(s): the data importer shall be one of the following:

Name: **ForgeRock US, Inc.**

Address: 201 Mission St, Suite 2900, San Francisco, CA 94105

Contact person's name, position and contact details: Chief Privacy Counsel, privacy@forgerock.com

Activities relevant to the data transferred under these Clauses: the activities specified herein.

Signature and date: n/a

Role (controller/processor/subprocessor): either processor or sub-processor (as the case may be)

Name: **ForgeRock Ltd**

Address: 4th Floor, Broad Quay House, Bristol, BS1 4DJ

Contact person's name, position and contact details: Chief Privacy Counsel, privacy@forgerock.com

Activities relevant to the data transferred under these Clauses: the activities specified herein.

Signature and date: n/a

Role (controller/processor/subprocessor): either processor or sub-processor (as the case may be)

(B) DESCRIPTION OF TRANSFER

(1) Categories of data subjects whose personal data is transferred

(A) Customer PII

The Customer may submit Customer PII to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to personal data relating to the following categories of data subjects:

#	Category
1.	Customer's employees and/or other staff members
2.	Customer's agents and/or, suppliers and/or other service providers
3.	Customer's end users and/or consumers and/or customers
4.	Any other individual who Customer invites to use the Services

(B) Customer Contact PII: individuals authorized by Customer to access Customer's account with ForgeRock.

(2) Categories of personal data processed

(A) Customer PII

The Customer may submit Customer PII to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of personal data:

#	Category
1.	Unique Universal Identifier/Username
2.	Email address
3.	IP address
4.	Telephone number
5.	Customer has discretion to configure the software to include other identifiers that are appropriate to its preferred use case, subject to ForgeRock's Identity Cloud Acceptable Use Policy

(B) Customer Contact PII: name, job title, email, address, IP address and telephone number

(3) Special categories of personal data

(A) Customer PII: Customer's preferred use case should not include identifiers that are deemed special categories of personal data.

(B) Customer Contact PII: ForgeRock does not contain special categories of personal data.

(4) Frequency of transfer (i.e. whether the data is transferred on a one-off or continuous basis)

(A) Customer PII: continuous

(B) Customer Contact PII: continuous

(5) Nature and purpose of the processing

(A) Customer PII

The objective of the processing of Customer PII by ForgeRock is the performance of the Services pursuant to the Agreement.

ForgeRock will process personal data as necessary to provide the Services under the Agreement.

ForgeRock does not sell Customer PII and does not share Customer PII with third parties for compensation or for those third parties' own business interests.

ForgeRock will process Customer PII as a processor in accordance with Customer's instructions as set forth in this Addendum.

(I) Specific nature of the processing: This will depend on the Services acquired by Customer.

Customer PII processing common to all services:

Application level support: including accessing application-generated debug and audit logs, which are available via customer trouble ticketing.

Customer PII processing specific cloud services:

Cloud Infrastructure level support: including access to the customer's cloud environment with respect to "Breakglass" support under our special access account privileges. Customer-initiated support requests will take place under an access account privilege provided by the customer. Any personal data access will be purely operational in nature.

Application level support: including accessing application-generated debug and audit logs, which are available via Google Cloud Operations Suite.Stack Driver

Back ups: including restoration of service to Customers in the event of interruption, primarily for disaster recovery purposes - backed-up data is encrypted at rest and ForgeRock has encryption key access.

Note: ForgeRock's access to Customer PII is operational in nature and scope because our activities are exclusively focused on providing Services.

(B) Customer Contact PII

ForgeRock will process Customer Contact PII as a controller in order to (a) manage the relationship with Customer; (b) carry out ForgeRock's core business operations, such as accounting and filing taxes; (c) detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; (d) perform identity verification; (e) comply with ForgeRock's legal or regulatory obligation; and (f) as otherwise permitted under Applicable Data Protection Law and in accordance with this Addendum, the Agreement, and applicable privacy notices.

(6) The period for which the personal data will be retained or if that is not possible, the criteria used to determine that period

(A) Customer PII

Customer Logs: any Software and/or Customer operating system logs that Customer may submit to the Services (for example via support tickets) will be retained for 6 months.

Customer's Cloud Environment: all Customer PII submitted to the Service (for example to configure ForgeRock's Identity cloud product) will be deleted 6 months after the cessation of the Agreement.

(B) Customer Contact PII

Retained for the duration of the Customer relationship and thereafter for a period of time enabling ForgeRock to maintain business records for audit purposes; comply with statutory record retention requirements; defend and/or bring existing or potential legal claims. Customer Contact PII will be deleted when no longer required for these purposes.

(7) For transfers to (sub) processors, also specify the subject matter, nature and duration of processing

Customer PII and Customer Contact PII: Details on ForgeRock's sub-processors and affiliates are set out here:

https://www.forgerock.com/resources/view/125449877/legal-document/privacy-documentation-sub-processor-affiliate-list.pdf

C. COMPETENT SUPERVISORY AUTHORITY

To the extent that GDPR applies to the Customer PII submitted to the Services, the Competent Supervisory Authority will be:

(1) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with GDPR as regards the data transfer shall act as competent supervisory authority.

(2) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

(3) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located shall act as competent supervisory authority.

SCHEDULE 2: TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Product Specific Security Terms

Technical and Organisational Security Measures for ForgeRock Identity Cloud and associated products and services:

Where Customer is executing a licence in relation to ForgeRock Identity Cloud and associated products and services (including 'hybrid products' the information security terms available at the following link shall apply:

https://www.forgerock.com/resources/legal-terms/forgerock-identity-cloud-security-documentation

Technical and Organisational Security Measures for **ForgeRock Identity Platform (self managed) software and associated and services**:

Where Customer is executing a licence in relation to ForgeRock Identity Platform (self managed) software and associated and services the information security terms set out below shall apply:

Information Security Overview

ForgeRock takes information security seriously.

This information security overview applies to ForgeRock's corporate controls for safeguarding personal data which is processed and transferred amongst ForgeRock group companies.

ForgeRock's information security program enables the workforce to understand their responsibilities.

Some customer solutions may have alternate safeguards outlined in the statement of work as agreed with each customer.

Security Practices

ForgeRock has implemented corporate information security practices and standards that are designed to safeguard ForgeRock's corporate environment and to address: (1) information security; (2) system and asset management; (3) development; and (4) governance.

These practices and standards are approved by ForgeRock's executive management and undergo a formal review on an annual basis.

Organisational Security

It is the responsibility of the individuals across ForgeRock's organisation to comply with these practices and standards.

To facilitate the corporate adherence to these practices and standards, the function of information security provides:

1. Strategy and compliance with policies/standards and regulations, awareness and education, risk assessments and management, contract security requirements management, application and infrastructure consulting, assurance testing and drives the security direction of the company.
2. Security testing, design and implementation of security solutions to enable security controls adoption across the environment.
3. Security operations of implemented security solutions, the environment and assets, and manage incident response.
4. Forensic investigations with security operations, legal, data protection and human resources for investigations including eDiscovery and eForensics.

Asset Classification & Control

ForgeRock's practice is to track and manage physical and logical assets.

Examples of the assets that ForgeRock's IT might track include:

1. Information Assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, archived information.

2. Software Assets, such as identified applications and system software.
3. Physical Assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment.

The assets are classified based on business criticality to determine confidentiality requirements.

Industry guidance for handling personal data provides the framework for technical, organisational and physical safeguards.

These may include controls such as access management, encryption, logging and monitoring, and data destruction.

Personnel Security

As part of the employment process, ForgeRock's staff undergo a screening process applicable per regional law.

ForgeRock's biennial compliance training includes a requirement for staff to complete an online course covering information security and data privacy.

The security awareness program may also provide materials specific to certain job functions.

Physical & Environmental Security

ForgeRock uses a number of technological and operational approaches in its physical security program in regards to risk mitigation.

ForgeRock's security team works closely with each site to determine appropriate measures are in place and continually monitor any changes to the physical infrastructure, business, and known threats.

ForgeRock's security team also monitors best practice measures used by others in the industry and carefully selects approaches that meet both uniqueness in business practice and expectations of data importer as a whole.

ForgeRock's security team balances its approach towards security by considering elements of control that include architecture, operations, and systems.

Communications & Operations Management

ForgeRock's security team IT organisation manages changes to the corporate infrastructure, systems and applications through a centralised change management program, which may include, testing, business impact analysis and management approval were appropriate.

ForgeRock's security team incident response procedures exist for security and data protection incidents, which may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

To protect against malicious use of assets and malicious software, additional controls may be implemented based on risk.

Such controls may include, but are not limited to, information security policies and standards, restricted access, designated development and test environments, virus detection on servers, desktop and notebooks; virus email attachment scanning; system compliance scans, intrusion detection monitoring and response, logging and alerting on key events, information handling procedures based on data type, e-commerce application and network security, and system and application vulnerability scanning.

Access Controls

Access to corporate systems is restricted, based on procedures to ensure appropriate approvals.

To reduce the risk of misuse, intentional or otherwise, access is provided based on segregation of duties and least privileges.

Remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place.

Specific event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

System Development & Maintenance

Publicly released third party vulnerabilities are reviewed for applicability in the data importer environment.

Based on risk to ForgeRock's business and customers, there are pre-determined timeframes for remediation.

In addition, vulnerability scanning and assessments are performed on new and key applications and the infrastructure based on risk.

Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk.

These processes enable proactive identification of vulnerabilities as well as compliance

Compliance

ForgeRock's information security, legal, privacy and compliance departments work to identify regional laws, regulations applicable to data importer compliance.

These requirements cover areas such as, intellectual property of the company and our customers, software licenses, protection of employee and customer personal information, data protection and data handling procedures, trans-border data transmission, financial and operational procedures, regulatory export controls around technology, and forensic requirements.

Mechanisms such as the information security program, Privacy council, internal and external review/assessments, internal and external legal counsel consultation, internal controls assessment, internal penetration testing and vulnerability assessments, contract management, security awareness, security consulting, policy exception reviews and risk management combine to drive compliance with these requirements.

SCHEDULE 3: JURISDICTION SPECIFIC TERMS

Australia

1. The term of "**Customer PII**" includes "**Personal Information**" as defined under Privacy Act 1988.
2. ForgeRock shall comply with the Australian Privacy Principles set out in Schedule 1 to the Privacy Act 1988 (other than Australian Privacy Principle 1).

Singapore

3. ForgeRock will process Customer PII to the standard of protection required by Personal Data Protection Act 2012 by implementing adequate technical and organisational measures as set forth in clauses 3.6 and 3.7 of this DPA.

United States

The following terms apply where ForgeRock processes Customer PII subject to the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("**CCPA**) including any regulations thereto, or by regulations adopted by the California Privacy Protection Agency:

4. the term(s):
   (a) "**data subject**" includes "**consumer**" as defined by the CCPA;
   (b) "**controller**" includes "**business**" as defined by the CCPA; and
   (c) "**processor**" includes "**service provider**" as defined by the CCPA.
5. The Customer:
   (a) appoints ForgeRock as a service provider to process Customer PII on behalf of the Customer;
   (b) discloses Customer PII to ForgeRock only for ForgeRock to perform the Services and for a valid business purpose; and
   (c) is responsible for ensuring that it has complied, and will continue to comply, with the requirements of the CCPA in its use of the Services and its own processing of Customer PII.
6. ForgeRock agrees that it:
   (a) will comply with obligations applicable to it as a service provider under the CCPA;
   (b) is prohibited from selling Customer PII or retaining, using or disclosing Customer PII except for the provision of the Services, or as otherwise permitted by the CCPA; and
   (c) will not sell or share Customer Content or retain, use, or disclose Customer PII outside of the direct business relationship between ForgeRock and Customer;
   (d) will not receive Customer PII as consideration for any Services provided to Customer;
   (e) will not process Customer PII for the purpose of providing services to another person or entity, except that ForgeRock may combine Customer PII received from one or more entities to which it provides similar services to the extent necessary to detect a Customer PII Breach and/or protect against fraudulent or illegal activity;
   (f) will provide Customer PII with the same level of privacy protection as is required by the CCPA; and
   (g) ensure that its agreement with any sub-processor complies with the CCPA, including, without limitation, the contractual requirements for service providers and contractors