(US) 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 capitalized 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 purposes of this DPA

1.1 "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations, as amended or superseded from time to time including, without limitation, as amended by the California Privacy Rights Act of 2020 ("CPRA");

1.2 The definition of **Customer PII** (as set out in the Agreement) shall be extended to include personal information relating to a Household (as defined in the CCPA)

1.3 Other capitalized terms not otherwise defined in this DPA or the Agreement shall have the definitions set forth in the **CCPA**.

2. **Customer Acknowledgement**: Customer acknowledges that ForgeRock and its Affiliates, and their respective agents 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 on-premise software (the "**Services**");

3. **Roles and Scope**:

3.1 This DPA applies to the collection, use, retention, disclosure, deidentification and/or reidentification ("**Processing**" and "**Process"**), and sale of Customer PII provided by Customer to ForgeRock to provide Services to Customer pursuant to the Agreement or to perform a Business Purpose;

3.2 Customer is a Business and appoints ForgeRock as a Service Provider to Process the Customer PII on behalf of Customer;

3.3 ForgeRock's Processing and/or sale of Customer PII for its own purposes independent of Customer's use of the Services specified in the Agreement are outside the scope of this DPA.

4. **Restrictions on Processing**:

4.1 ForgeRock is prohibited from Processing the Customer PII for any purpose other than for the specific purpose of performing the Services specified in the Agreement for Customer, as set out in this DPA, or as otherwise permitted by the CCPA;

4.2 ForgeRock shall not further Process and/or sell the Customer PII except as necessary to perform the Business Purpose;

4.3 ForgeRock warrants that it will not use the Customer PII it receives from or collects on behalf of Customer in violation of the restrictions set forth in the CCPA.

4.4 ForgeRock shall not Process the 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 Customer PII security incidents, or protect against fraudulent or illegal activity.

5. **Customer's Warranty**: Customer warrants that it shall comply with its obligations under applicable data protection law including but not limited to:

5.1 providing ForgeRock with only those sets of Customer PII that are essential, relevant and adequate for the purposes of the ForgeRock providing the Services, under general data minimisation principles;

5.2 providing Consumers with appropriate privacy notices;

5.3 obtaining any required consents from Consumers; and

5.4 ensuring there is a lawful basis for ForgeRock and its sub processors or Affiliates to process Customer PII or by implementing any other lawfully required activity to assure adherence.

6. **Notice**: Customer represents and warrants that it has provided notice that the Customer PII is being Processed or shared consistent with Cal. Civ. Code 1798.140(t)(2)(C)(i).

7. **Consumer Rights**:

7.1 ForgeRock shall provide commercially reasonable assistance to Customer in facilitating compliance with Consumer rights requests;

7.2 Upon direction by Customer, and in any event no later than 30 days after receipt of a request from Customer, ForgeRock shall promptly delete the Personal Information as directed by Customer;

7.3 ForgeRock shall not be required to delete any of the Customer PII to comply with a Consumer's request if it is necessary to maintain such information in accordance with Cal. Civ. Code 1798.105(d), in which case ForgeRock shall promptly inform Customer of the exceptions relied upon under 1798.105(d) and ForgeRock shall not use the Customer PII retained for any other purpose than provided for by that exception.

8. **Deidentified Information**: In the event that either Party shares Deidentified Information with the other Party, the receiving party warrants that it has implemented:

8.1 technical safeguards that prohibit reidentification of the Consumer to whom the information may pertain;

8.2 business processes that specifically prohibit reidentification of the information;

8.3 business processes to prevent inadvertent release of Deidentified Information; and

8.4 will make no attempt to reidentify the information.

9. **Information Security Measures**: For the duration of the Agreement ForgeRock shall comply with the measures set forth in Appendix 1, which is hereby incorporated into this DPA.

10. **Mergers, Sales, or Other Asset Transfers**: In the event that either party transfers to a Third Party the Customer PII as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the Third Party assumes control of all or part of such party to the Agreement, that information shall be used or shared consistently with applicable law. If a Third Party materially alters how it uses or shares the Customer PII in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the Consumer in accordance with applicable law.

11. **As Required by Law**: Notwithstanding any provision to the contrary of the Agreement or this DPA, ForgeRock may cooperate with law enforcement agencies concerning conduct or activity that it reasonably and in good faith believes may violate federal, state, or local law.

12. **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.

13. **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.

(US) Data Processing Addendum

APPENDIX 1: DESCRIPTION OF FORGEROCK'S TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

ForgeRock 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 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 executive management and undergo a formal review on an annual basis.

Organizational Security

It is the responsibility of the individuals across the organization 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 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, organizational 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, employees undergo a screening process applicable per regional law. ForgeRock's biennial compliance training includes a requirement for employees 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. Their 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. They also monitor best practice measures used by others in the industry and carefully select approaches that

meet both uniqueness's in business practice and expectations of ForgeRock as a whole. ForgeRock balances its approach towards security by considering elements of control that include architecture, operations, and systems.

Communications & Operations Management

The IT organization manages changes to the corporate infrastructure, systems and applications through a centralized change management program, which may include, testing, business impact analysis and management approval were appropriate.

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 ForgeRock's environment. Based on risk to ForgeRock's business and customers, there are predetermined 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

The information security, legal, privacy and compliance departments work to identify regional laws, regulations applicable to ForgeRock 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.