ForgeRock

ForgeRock Identity Cloud

› **Privacy Data Sheet**

ForgeRock Identity Cloud

The ForgeRock Identity Cloud is a comprehensive, extensible, and customizable identity platform as a service designed to help organizations leverage a single platform for all identity needs–consumers, workforce, and things.

We secure, monitor, and run the software while providing the flexibility and extensibility to satisfy some of the most complex identity and access management use cases in the industry.

ForgeRock Identity cloud supports all major identity standards, including OAuth 2.0, OIDC, SAML, and CIBA. The solution also provides synchronization and storage. The ForgeRock Identity Cloud can be supplemented with ForgeRock Identity Gateway or ForgeRock Agents or ForgeRock Autonomous Identity to provide policy enforcement and application programming interface (API) management and security.

Protecting your data and privacy are important to us. This document summarizes the data protection and privacy aspects of the ForgeRock Identity Cloud.

Further details on the information security aspects of the ForgeRock Identity Cloud are available at: https://www.forgerock.com/resources/view/107430026/whitepaper/forgerock-identity-cloud-security-whitepaper.pdf.

Please see our Data Processing Addendum and Acceptable Use Policy at https://www.forgerock.com/terms for further details.

Personal Data Processing

This table highlights the personal data processing activities associated with ForgeRock Identity Cloud:

Data Subject Category	Personal Data Sets	Processing Purpose(s)	Our Status/ Access Level
Customer Staff	› Name › Email address › IP address › User ID	› Account registration › User profile › Authentication › Authorization	**Data Controller**
Customer End User	Data sets are Customer configurable within the cloud environment and may include: › Name › Email address › IP address 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 Accepted Use Policy	**Cloud Infrastructure-Level Support:** Involves access to the customer's cloud environment with respect to: › "Breakglass" support under our special access account privileges › Customer-initiated support requests under an access account privilege provided by the customer **Application-level Support:** Involves access to application-generated debug and audit logs, which are available to us via: › Stack Driver (our log aggregator tool) › Customer trouble ticketing **Back-up:** Involves restoring service to customers in the event of interruption, primarily for disaster recovery purposes Back-ups are encrypted at rest. We have encryption key access for the purposes of providing disaster recovery services **Professional services:** Involves accessing the customer's cloud environment with respect to customer-initiated support requests around application setup and configuration, via customer-provided account privileges	**Data Processor** Access is *operational* in nature and scope because our activities are exclusively focused on providing services.

Cross-Border Transfers

Customer's Staff

The personal data of new customer's staff will be stored in a database location selected by you, and a privacy notice (compliant with applicable law) will be delivered to each new customer staff member at the point of personal data capture.

Customer's End Users

When a new customer accesses ForgeRock Identity Cloud, the customer's information (including end user personal data) is systematically created, processed and stored in the location designated by you.

You will engage in cross-border data transfers when our support teams (primarily based in Bristol, UK; San Francisco, California; Austin, Texas; Singapore; and Australia) access your end user and other personal data to provide the services described in Section 2 above.

ForgeRock Identity Cloud relies on third-party cloud hosting service providers with data centers based in various global locations. We also rely on IT service providers that provide cloud services, and we leverage EU Standard Contractual Clauses with respect to all international data transfers.

A list of third-party service providers is available upon request.

Access Control

Our access to your personal data is highlighted in the following table:

Personal Data Category	Access Privileges	Purpose(s)
Registration Information	Our employees/staff, including sales, administration, enterprise security, customer success, and engineering teams	› Account creation › Product enablement and use › License entitlement validation › Customer notifications › General product support and operations
Customer End User Information	Our employees/staff, including enterprise security, customer success, engineering, and professional services teams	› Breakglass support under ForgeRock Special Access Account privileges › Customer-initiated support /maintenance requests under an Access Account privilege provided by customer › Security monitoring › Analysis of debug and audit logs for application support purposes › Back-ups and disaster recovery › Professional services (if utilized by customer)

Further information with respect to technical and organizational measures around employee/staff security are available at: https://www.forgerock.com/resources/view/107430026/whitepaper/forgerock-identity-cloud-security-whitepaper.pdf

Data Retention and Deletion

Personal Data Category	Retention Period	Retention Reason(s)
Registration Information	60 days after a customer's Identity Cloud agreement has ceased or terminated	› Post-service notifications › Customer change control
Customer End User Information	60 days after a customer's Identity Cloud agreement has ceased or terminated	› Customer change control

Security

We align security practices to meet or exceed industry good practice and have achieved industry recognised standards such as ISO27001 in order to ensure the confidentiality, integrity, and availability of systems and data. We also validate these programs on an ongoing basis via (a) internal audits, (b) independent external audits, and (c) certification bodies.

Security Incident and Breach Notification

We operate an ISO-certified Incident Response program, facilitating rapid identification, isolation, and remediation of security incidents. As part of the program, ongoing assessments are made for the impact of events on the confidentiality of personal data to ensure that customers are notified without delay in the event of a personal data breach.

The incident and breach processes are overseen by our Chief Information Security Officer, who oversees critical incidents, as well as ensuring review and testing of the incident response and breach response programs on an ongoing basis.

Further Information

If you like to discuss any aspect of ForgeRock's technical and organizational measures around our product's privacy controls please contact ForgeRock's Chief Privacy Counsel at privacy@forgerock.com.