ForgeRock Autonomous Access

ForgeRock Autonomous Access leverages artificial intelligence (AI) and machine learning (ML) techniques to analyze threat signals and anomalous behavior patterns. It speeds up and simplifies access decisions, enabling your organization to block threats and deliver personalized journeys that enhance the digital experience of legitimate users.

ForgeRock Autonomous Access is available as part of the ForgeRock Identity Cloud stack, the leading identity and access management cloud solution.

Personal Data Processing

This table highlights the personal data processing activities associated with ForgeRock Autonomous Access:

Data Subject Category	Personal Data Set	Processing Purpose(s)	Our Status/ Access Level
Customer End-User Information	Data sets are customer-configurable within the cloud environment and may include: › Name › Email address However, the product does automatically pick up specific end- user data sets including: › User ID › IP address	**Threat Visualization and Analytics** via extraction of personal data from logs generated by ForgeRock Identity Cloud and analysis of such logs in real time within customer's ForgeRock Identity Cloud tenant **Cloud Infrastructure-Level Support** for access to your isolated cloud tenancy with respect to: • "Breakglass" support under our special access account privileges; • Support requests that you initiate under an access account privilege provided by you. **Application-Level Support** for access to application-generated debug and audit logs, which are available to us via: • Google's Cloud Operations Suite, which is our log aggregator tool; • Support request ticketing. **Backup** for restoring service to you in the event of interruption, primarily for disaster-recovery purposes. Backups are encrypted at rest. We have encryption key access for the purposes of providing disaster-recovery services. **Professional Service**s for accessing your isolated cloud tenant with respect to support requests initiated by you around application setup and configuration via specific account privileges provided by you.	Data Processor

Cross Border Transfers

Customer's End Users Personal Data: When a 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 the customer. Logs generated by ForgeRock Identity Cloud are then analyzed by ForgeRock Autonomous Access, identifying behavior patterns and providing real-time analysis of likely threats.

Whenever a risky authentication attempt is detected, logs generated by ForgeRock Autonomous Access are sent to and analyzed by Elasticsearch, ForgeRock's sub-processor, for visualization purposes (please see above). Your instance of Elasticsearch's software is located within the same GCP tenant as your instance of ForgeRock Identity Cloud, so no data ever leaves your environment.

You will engage in cross-border data transfers when our support teams (based in the EU and the U.S.) access your end-user and other personal data to provide the services described in Section 2 above.

ForgeRock Autonomous Access 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. ForgeRock Autonomous Access primarily relies on assistance from service providers based in the United States.

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

Access Controls

Personal Data Category	Access Privileges	Purposes
Customer End-User Personal Information	Our employees/staff, including enterprise security, customer success, engineering, and professional services teams	Account creation. Product enablement and use. License entitlement validation. Customer notifications. General product support and operations.

Data Retention and Deletion

Personal Data Category	Retention Period	Retention Reason(s)
Customer End-User Personal Information	ForgeRock Autonomous Access – six (6) months after the receipt of logs from ForgeRock Identity Cloud	To allow ForgeRock Autonomous Access to learn the patterns of customer end-user logins
Customer End-User Personal Information	Elasticsearch – three (3) months after receipt of logs from ForgeRock Autonomous Access	To provide threat visualization and analytics

Security

We align security practices to meet or exceed industry good practices 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 regarding 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 ensures review and testing of the incident response and breach response programs on an ongoing basis.

Further Information

If you would 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**.

More details on Elasticsearch's security posture can be found **here**. Elasticsearch was assessed under our rigorous procurement processes, which included detailed Third-Party Risk Assessments for Privacy and Information Security. Additionally, ForgeRock has bound Elasticsearch to appropriate contractual terms, which include the EU Standard Contractual Clauses.