Customer Data “Privacy First” in Automation Anywhere Cloud

The Automation Anywhere® cloud portfolio is a hosted service delivery platform. The cloud portfolio includes an integrated Control Room and bot-creation capabilities hosted in the cloud, along with the ability to run the cloud-connected Bot Runner nodes on the customers' infrastructure. Additional products, such as IQ Bot™, can also be hosted in the cloud.

The cloud offering is designed to ensure data privacy and operates following GDPR and other data privacy principles and guidelines.

DATA SECURITY

The deployment architecture adopts a "privacy first" approach for the protection of customers' data and infrastructure.

Data connectivity between the Bot Runner on the customer network and the Control Room that resides in the cloud is encrypted. Secure encryption protocols like HTTPS and TLS 1.2 are used for encrypting data in motion. For data that is stored in the cloud, data at rest encryption (e.g., AES 256-bit encryption) is used.

The full security posture, covering the cloud operations upon which the cloud offering is deployed, encryption technologies, and the network security of the environment, are described in the Cloud Security Operations Guide.

DATA COLLECTION

The deployment model involves customers building their bots and managing the bot deployments from the Control Room in the cloud. Once the bots are built, they are tested and deployed for execution on the users' own compute infrastructure.

The table below describes the data collected for the Automation Anywhere cloud portolio. The table provides guidance on which data could possibly be used to identify a natural person.

Data Item	Data Category	Description
Username	Personal	email, First and Last name, preferred name, time zone, last log in, password, questions set, AD-domain
User password	Personal	
Password security key	Personal	Credential Vault password security key
Bot Runer device access	Personal	Device username and access credentials
Role definitions	Personal	Admin, creator, etc.
Roles mapped to users, device, resource	Personal	User roles
Bot device IP / FQDN	Personal	Device IP address or FQDN can be tracked to a user
Bot definition (repository)	Metadata	Data stored as part of the bot definition
Bot application credentials	Personal	Application user, URL, public key, routing name
Control Room bot schedules	Metadata	Bot management; When and where to run bots
WLM workflow definition	Metadata	When and where to run bots in which sequence
Audit logs	Personal	May contain identifiers: device message log, deployment message log, email message log, job execution log: (start/end time, user ID, schedule, automation name, deployment ID. Device name, bot name, user name), user management edit log, Credential Vault message log, server & data base change logs
Errors logs	Personal	May contain identifiers
Operational analytics	Metadata	Service status
Usage data	Metadata	Feature usage, licenses enabled, aggregated with no personal/user data identifiers. For IQ Bot: users learning instances, domains, operational statistics, validation changes, uploaded documents, and extraction results.
Usage data	Personal/ Metadata	Users learning instances, domains, operational statistics, validation changes, user uploaded documents, and extraction results.

DATA USE

Operation and Support

Cloud operations will monitor deployment systems and operational performance in order to operate, scale, and support the service.

When support services need access in order to troubleshoot and resolve issues, support personnel will only do so with the appropriate customer permission.

In order to improve the product, Automation Anywhere will:

- Analyze feature usage data to improve the product—e.g., add telemetry to provide operational visibility into feature usage. This will help Automation Anywhere to prioritize and add improvements in the product. Examples include:
  - Review frequency of usage of Excel commands to help prioritize which commands to add to future releases
  - Provide operational best practices recommendations
  - Provide support services that will be used for updating, securing, and troubleshooting
  - Personalize products and make recommendations
  - For IQ Bot, customer data will be used to improve quality of AI learning skills

For more information about Automation Anywhere data privacy policy please refer to: https://www.automationanywhere.com/in/privacy

Data Retention After Subscription Termination

Automation Anywhere will keep customer data, configs (bots), IQ Bot data, and most logs for 30 days after the customer's subscription ends.Some logs may be kept for up to 180 days after the customer's subscription ends.

Full details of the Data Processing Addendum and data retention policy can be found here: https://www.automationanywhere.com/support/DPA.pdf

DATA PROTECTION

Automation Anywhere has a comprehensive set of security features that either automatically provide or are configurable by design to provide data protection. As with any enterprise application, the consistent and proper utilization of security controls depends upon the organization utilizing the enterprise application. Authorization of users is dependent upon the IT administrators, who should implement controls to ensure that only authorized personnel have access.

The data owner should ensure that only authorized personnel with a business need can access the service. Corporate users with access can be granted fine-grained permissions via role-based access controls (RBAC). The RBAC models assure dual-controls and separation of duties within the operations. Permissions can be implemented for all aspects of product operation, including credentials, bots, Bot Runners, Bot Creators, bot schedules, IQ Bot learning instances, audit log access, workload management queues, and pools.

Automation Anywhere provides full audit capabilities where all user actions are audited within the platoform, providing records of all access and actions taken by operations personnel. Audit is automated for all privileged and non-privileged roles to conform to best practices as defined in NIST AC-6.

As bots are software programs developed by customer business experts, state-of-the-art required Secure Software Development Life Cycle (SDLC) processes must be implemented by the customer accordingly. Toward this end, Automation Anywhere supports separation of development, testing, and production environments through a combination of separate deployments and RBAC as described above.

Pseudonymization

GDPR specifically calls out pseudonymization as an appropriate technical measure to protect data. Pseudonymization transforms data to artificial identifiers. This gives the Controller and Processor a way to process data such that it is no longer possible to use the data to identify a natural person without additional information that is held separately. Tokenization is another approach that transforms data such that it can be referenced later but in terms of the tokenized data such that it cannot be used to identify a natural person.

Automation Anywhere recommends the use of pseudonymization of data for development and testing environments. For IQ Bot, documents and images in production environment will be processed with actual user information. There is no technical possibility to pseudonymize these documents automatically and use IQ Bot.

Data Remanence in Control Room

There are instances where data is retained within the databases which support the Control Room. Specifically, when using workload management, IQ Bot and Bot Insight™ (future release). In all cases regarding data remanence in Control Room, pseudonymization and tokenization reduce Controller and Processor entity effort to comply with GDPR. Also, when enabling logs for debugging information, such as username (users of the platform), it will be retained in the logs.

Workload Management and Queues

When utilizing workload management (future release) to deploy multiple bots for the same automation, the work items that are placed into the queues are stored in the Control Room database. Through the Control Room user interface, any work item may be queried, reviewed, and deleted. When processing personal data in work items, queues can be periodically deleted.

User credentials can be added and deleted by any administrator with the appropriate privileges, set by the appropriate role. The Control Room supports the querying, reviewing, and deleting of any credential at any time.

The Control Room provides the means to set up and remove user accounts with appropriate RBAC controls. The organization's administrator is responsible for providing appropriate access to users and resources. The administrator should create a policy with required level of access as per corporate and user data privacy guidelines. If an individual user requests access or limitations to their personal information, they should contact the customer's administrator. The customer's administrators can delete the user's accounts in the Control Room.

For more detail with respect to GDPR data privacy inquiries and copies of the personal data, Automation Anywhere provides the following site Data Subject Access Rights Request Form.

SUMMARY

Today's cloud-based, business-critical offerings are entrusted with delivering solutions with access security and data privacy as paramount considerations from the ground up.

The Automation Anywhere cloud portfolio is designed to meet and exceed demanding operational guidelines, and for good reason: we care deeply about customer privacy and security in delivering automation to customers.