Katalon Data & AI Trust FAQs

Last updated: November 7, 2025

This document provides answers to common questions about how the Katalon Platform handles your data, including details on our product-specific data processing, privacy practices, security controls, and the use of artificial intelligence (AI). We know that your data is a critical asset, and our commitment is to handle it securely and transparently, while providing powerful AI capabilities you can trust.

This FAQ is for informational purposes only and does not amend or form part of any contract with Katalon. The information is subject to change as our products and AI features evolve. For more detailed information, please refer to the Katalon Trust Center and your specific agreement with Katalon.

I. SECURITY

1. Do you have a formal information security program?

- Yes, Katalon operates an enterprise-wide **Information Security Management System (ISMS)** aligned to **ISO/IEC 27001:2022** and mapped to **NIST CSF** and **ISO/IEC 27017:2015** (cloud). The program is **CISO-led**, **independently assessed**, and enforced through a defense-in-depth control stack covering access control, data protection, secure SDLC, logging & monitoring, vendor risk, IR/BC/DR, and more. All staff complete security onboarding, annual training, and yearly policy re-acknowledgements.

2. What security certifications and frameworks does Katalon follow?

- Katalon is **ISO/IEC 27001:2022** aligned and **SOC 2 Type II** attested. Our cloud controls are mapped to **ISO/IEC 27017:2015**, with program governance anchored in **NIST CSF**. We also embed GDPR/CCPA obligations via our **Personal Data Management** and **Data Protection** standards and run continuous risk assessment against our control catalog.

3. How is security governed at Katalon?

- Security is led by our **Chief Information Security Officer (CISO)**, with executive sponsorship and cross-functional ownership (Engineering, CloudOps, Legal/DPO, GRC). Governance runs on a **Plan-Do-Check-Act** cadence: quarterly risk

reviews, control testing, tabletop exercises, vendor reviews, and board-level reporting. Policies are reviewed at least annually; exceptions follow a formal risk-acceptance workflow.

4. **How is user data stored? What encryption is used for data at rest and data in transit?**
    - Data is stored within approved data stores within AWS. Structured data is stored within databases and unstructured data is stored within securely configured AWS S3 buckets.
    - AES 256-bit and TLS 1.2+ (RSA 2048-bit) encryption is enabled for data at rest and in transit respectively. Approved secure channels include SSH, HTTPS, and SFTP.
    - Further, sensitive records are hashed SHA256 at the database table level.
5. **What controls does Katalon have in place to protect personal data (PII)?**
    - Katalon safeguards PII through an enterprise ISMS (ISO/IEC 27001:2022) and SOC 2 Type II (including the Privacy criteria), with DPO/ and CISO oversight. Controls include: data minimization & classification, encryption at rest and in transit, least-privilege/RBAC with quarterly access reviews and time-bound production access, centralized logging & monitoring, and a tested Incident Response, BC/DR, and secure SDLC program. We enforce retention & deletion via documented schedules and honor DSARs. Vendors undergo security and privacy due diligence with contractual safeguards (incl. SCCs where applicable). AWS hosting uses logical tenant isolation and high availability.
    - Our Data Processing Addendum (DPA) is available for review at https://katalon.com/terms#dpa.
6. **Does Katalon depend on any cloud providers to support customer services?**
    - Yes, the Katalon platform uses Amazon Web Services (AWS) for all production infrastructure and storage.
7. **Does Katalon have a disaster recovery plan (DRP) and business continuity plan (BCP)?**
    - Yes, Katalon systems are hosted on AWS, leveraging the platform's native services to ensure continuity and redundancy. Regular backups and snapshots are taken and thoroughly tested to safeguard data. Additionally, the systems are designed and architected with high availability as a key focus.

II. PRIVACY & DATA USE

1. **What types of data does Katalon process, and where can I find the details?**

   We are committed to transparency about the data we process to provide and improve our services. We categorize the data into two main types:

   - **Service & Account Data**: To manage your account, provide billing, and ensure the security and operation of our services, we process necessary information like user emails, subscription details, and IP addresses.
   - **Customer Content**: This is the data you generate and manage within the Katalon Platform, such as your test scripts, test artifacts, and other data you provide to the AI features ("**Your Data**"). **You own and control this data.** For our cloud products, this data is stored and processed in our secure AWS cloud environment in the USA. For on-premise deployments, “Your Data” remains on your infrastructure.
   - Our commitment is to collect only the data necessary to deliver and enhance the service you've entrusted to us.

2. **Where to Find Detailed Information?**

   For a complete and legally binding description of our data processing activities, including specific data types, purposes, storage locations, and retention periods for each product, please refer to our official documents:

   - Our Privacy Policy provides full details on how we process Service & Account Data.
   - Our Data Processing Addendum (DPA) governs how we process Customer Content (“Your Data”) on your behalf.

   These documents serve as the single source of truth for our data handling practices.

3. **How does TrueTest process and protect sensitive user data captured from production environments?**

   Protecting customer data is a foundational principle of TrueTest's design. We employ a multi-layered, defense-in-depth strategy centered on **data minimization** and **privacy-by-design** to ensure that Personally Identifiable Information (PII) and other sensitive data are never captured, processed, or stored. Our approach gives you comprehensive control and transparency.

Here's a breakdown of the safeguards we have in place:

- **Proactive Data Filtering at Source**: Our primary line of defense is the TrueTest Agent, which filters all data on the client-side *before* it is ever transmitted to the Katalon backend. This ensures sensitive information never leaves your environment.
    - **Automated PII Redaction**: The agent is pre-configured to automatically detect and redact common sensitive data patterns using regular expressions (regex). This includes, but is not limited to:
        - Social Security Numbers
        - Email and IP addresses (IPv4 & IPv6)
        - Phone numbers and zip codes
        - Credit card details (number, CVC, expiration)
        - Passwords (by detecting "password" input field types)
    - **Customer-Controlled Exclusion**: You have granular control to prevent the capture of any specific data. By simply adding the katalon-excluded CSS class to any UI element, you can instruct the agent to completely ignore it and its contents. This allows you to tailor data exclusion to your unique application and business needs.
- **Backend Verification and Security**: As a secondary safeguard, we implement security measures on our backend to verify that the initial, client-side filtering was successful.
    - **Ingestion Scanning:** All data received from the TrueTest Agent undergoes an immediate secondary scan upon ingestion. In the unlikely event that any sensitive data patterns were missed by the agent, they are identified and purged *before* being processed or stored.
    - **Continuous Monitoring:** We leverage industry-leading cloud security tools, such as AWS Macie, to routinely scan our systems and provide an additional layer of protection and verification against sensitive data exposure.

By combining automated, client-side redaction with customer-controlled exclusions and robust backend verification, TrueTest is designed to ensure that the user interaction data used for test generation is anonymous, secure, and free of sensitive information.

4. **Does Katalon use customer data to train third-party AI models?**

   No. We do not use your data to train our proprietary AI models or any third-party AI models. This commitment is a foundational principle of our AI services and is contractually enforced with our sub-processors. Our agreements with AI service providers, like Microsoft Azure OpenAI, explicitly require that your data is not logged or retained for model training purposes.

5. **What controls do I have over AI features and how my data is used?**

   We believe in providing you with complete and granular control over AI functionality and data usage.

   - **Platform-Wide AI Control:** As an administrator, you can enable or disable all AI services across your entire Katalon account with a single toggle in the Admin settings. Disabling this turns off all AI-powered features, including TrueTest and generative capabilities.
   - **Bring Your Own AI (BYOAI):** For maximum flexibility and to align with your organization's specific data governance policies, you can configure Katalon's AI features to use your own AI provider subscriptions:
     - **For Katalon Studio & TestOps**: You can easily integrate features like StudioAssist and Manual Test Generation by providing your own API key for your preferred AI provider.
     - **For Katalon TrueTest**: You can configure TrueTest to process data through your own private instance of Microsoft Azure OpenAI. Our engineering team will partner with yours to ensure a seamless integration.

6. **What is Katalon’s protocol for responding to security incidents related to TrueTest?**

   We maintain a rigorous, multi-stage incident response (IR) protocol managed by our dedicated internal Security Team. Given TrueTest’s potential interaction with production environments, it is governed by our highest-level response priority. Our protocol is structured as follows:

- **Detection & Analysis**: We use comprehensive, auditable logging and continuous monitoring across all platform components to rapidly detect and analyze anomalous activity.
- **Containment & Remediation**: Upon confirming an incident, the Security Team immediately works to contain the impact and remediate the vulnerability. Incidents are triaged and addressed according to a strict severity matrix, with defined response SLAs based on potential impact.
- **Notification**: In the event of a security incident affecting your data, we will provide prompt notification to your designated account contacts in accordance with our contractual obligations and applicable laws.

If you suspect a security issue, please report it immediately via the Katalon Support Portal for the fastest response.

7. **How can I request the deletion of my data?**

   We provide clear pathways for data deletion:

   - **Self-Service Deletion:** You can delete specific content, such as projects, test suites, and test cases, directly from your account at any time.
   - **Full Account Deletion:** To permanently delete your entire account and all associated data, you can submit a formal request through the Katalon Support Portal. Our team will process the request in accordance with our data retention policies.
8. **How do you select and manage third-party vendors (sub-processors) who process our data?**

   We have a robust vendor management program, which is audited annually as part of our SOC 2 Type II certification. This program ensures any third party that processes customer data meets our high security and privacy standards.

   - **Due Diligence:** Before onboarding, all vendors undergo a formal risk assessment of their security and privacy posture, including a review of independent certifications like SOC 2 and ISO 27001.

- **Contractual Safeguards:** We execute binding Data Processing Agreements (DPAs) with all sub-processors, ensuring they adhere to data protection standards equivalent to our own.
- **Full Transparency:** We maintain a public list of our sub-processors that details what services they provide and where they are located.

III. TRANSPARENCY & GOVERNANCE

1. How does Katalon label AI-generated content?

To ensure full transparency, we clearly identify content generated by AI:

- **Katalon TrueTest:** Test cases generated by TrueTest are automatically attributed to “Katalon AI” as the creator and are organized into designated “AI-Generated” folders.
- **Katalon Studio & TestOps:** AI-generated assets, like test cases, are automatically tagged with “GenAI” in their properties. Please note that if you copy raw content from a feature like the StudioAssist chat window, this label is not automatically carried over.

2. Who owns the intellectual property (IP) generated by Katalon's AI features?

The short answer is: **You own it.**

Our policy is designed to be straightforward. Under our Customer Terms of Use, we define both the content you provide to the AI (Inputs) and the test scripts or other content the AI generates in response (**Outputs**) as “Your Data.” You retain full ownership of and control over Your Data.

However, it's important to understand a few key aspects inherent to using generative AI:

- **Your Responsibility**: Just as you own the Output, you are also responsible for its use. This includes ensuring that your Input and your use of the Output do not violate any laws or third-party rights.
- **Outputs Are Not Exclusive**: Because AI models learn from vast datasets, the Output they generate is not guaranteed to be unique. It's possible for other users to receive similar or identical Outputs in response to their own Inputs.

- **Our Commitment to Your IP**: We will never use your Inputs or Outputs to train our AI models for other customers. Your intellectual property remains yours and is not used to enhance our services for others.

3. **How should my team approach using the output from Katalon's AI features?**

   We design our AI features to be a powerful co-pilot for your team, accelerating your testing lifecycle and boosting efficiency. Like any advanced tool, it's best used with a clear understanding of its capabilities and limitations. We recommend the following best practices:

   - **Treat AI as a "First Draft" Expert:** AI-generated output, such as test scripts or code, should always be reviewed, validated, and tested by a qualified member of your team before being implemented in a production environment.
   - **You Are the Final Authority:** You and your team are the experts on your application and its specific context. You are ultimately responsible for the final test scripts and any other content you decide to use.
   - **Understand the Nature of AI:** Due to the way large-scale AI models work, the output you receive may not be unique, and other users may receive similar outputs.

   Our goal is to empower your team with cutting-edge tools while ensuring you remain in full control. For the specific legal terms governing the use of AI features, including disclaimers and acceptable use policies, please refer to our **Customer Terms of Use**.