capriza Data & Security

Our Security Principles

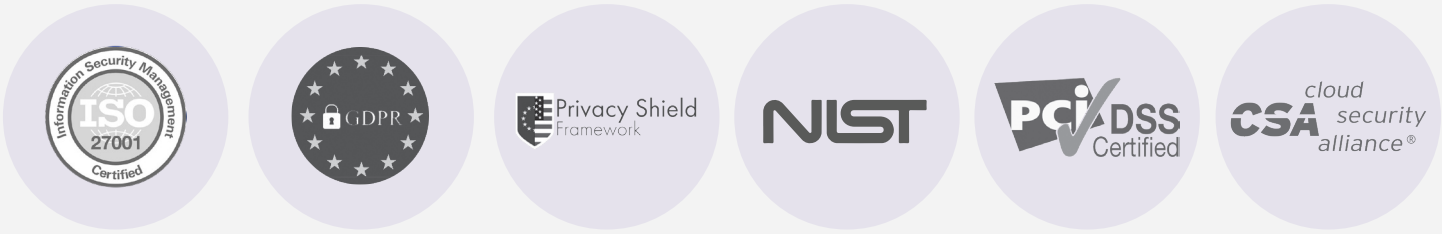
1. Secure and Private Data Policies.

We don't collect any data unless we're authorized to do so by you. We don't store any personally-identifiable customer information without masking, unless explicitly instructed by you to fulfill a particular use case. All data, whether at rest or in transit, is encrypted with **state-of-the-art encryption policies and technology**, and only Capriza developers and customer success managers have access to whitelisted data.

Capriza has an exceptionally lengthy data security track record, with over eight years of doing business across hundreds of customers and all geographies around the world.

2. Enterprise-grade Certification and Regulation.

Capriza holds the following enterprise-grade security certifications and adheres to the following regulations:



3. Ongoing Security Testing and Certification.

As part of our continual security review, we undergo **periodic penetration testing and vulnerability scanning** to ensure we're keeping your data safe and secure. Twice a year, Capriza undergoes a third party audit by ComSoc Global that includes pen testing on both an app and infrastructure level, as well as detailed architecture and code reviews. Their testing produces a regular and updated report, which we're delighted to share our customers and prospective customers under NDA.

Capriza also ensures the highest standard of developer security training, adhering to the **Open Web Application Security Project** (OWASP), a once-yearly program to ensure that we continue to write the most secure, enterprise-grade code.