GDPR: Security & Compliance

BRIEF

GDPR: The Basics

The GDPR is a comprehensive data protection law that updates and replaces the Data Protection Directive 95/46/EC for all EU member states. It's designed to strengthen the protection of "Personal Data" (any information relating to an identified or identifiable natural person, or "data subjects"). Compliance is mandatory for any organization if they are offering goods or services (whether paid or free) to EU data subjects (data subjects are defined as EU citizens or EU residents) or monitoring the behavior of EU data subjects within the EU.

How Will Qubole Comply with the GDPR?

Qubole is fully prepared for the GDPR. We understand the complexities of GDPR compliance and we are committed to using our domain knowledge and best practices to help you meet GDPR.

Note: For more detailed information about how Qubole meets GDPR compliance, please refer to our whitepaper, *GDPR: Security and Compliance*

Specifically, Qubole will also continue to enhance data protection and compliance in these areas:

Accountability

Data Protection Officer (DPO) Qubole employs a Chief Security Officer (CSO) who functions as the organization's top executive responsible for security. Our CSO also serves as our DPO under the GDPR requirements.

Policies and Procedures

Qubole maintains a set of security policies, standards and procedures that provide our workforce with stringent data protection and compliance guidelines. Our Data Protection Policy Addendum and Agreement supports our commitment to this important legislation and is available here.

Mandatory GDPR Security Awareness Training

All Quboler’s have taken mandatory GDPR compliance training. Further job-specific training will be required for individuals with responsibilities related to GDPR compliance.

Compliance and Risk Activities

Qubole evaluates the design and operation of the Qubole platform, including all services, applications and processes to ensure compliance with internal and external standards. We engage credentialed assessors to perform external audits at least once per year including Privacy Shield. Qubole engaged with TrustArc (formerly TRUSTe) to complete and attest to compliance with the US Privacy Shield regulation around privacy and transfer of EU Personal Data to the United States and now works with them for arbitration and notification services.

3rd Party Innovation

Qubole has partnered with 3rd party GDPR organizations specializing in providing translation and assistance with the practical application of the GDPR to our unique business model.

Data Protection and Other Security Measures

GDPR regulations mandate that personal data is kept confidential and secure. Qubole’s maintains a staff of security practitioners dedicated to ensuring that all systems (IT, Development, and Customer Support) remain secure and confidential at all times.

Any sensitive or confidential information will only be shared with authorized users.

What are your obligations under the GDPR as a QDS User?

Similar to our existing legal requirements, GDPR compliance requires a partnership between Qubole and our customers in their use of our services. When you use a cloud provider, they are responsible for securing the underlying infrastructure that supports the cloud, and you are responsible for anything you put on the cloud or connect to the cloud. This model of shared security responsibilities also applies to Qubole as a service provider and your role as a QDS user.

Customer	Qubole	Cloud Provider (AWS, Azure, Oracle Cloud)
Responsible for user access management and data security in the cloud	Responsible for security of the platform and big data service in the cloud	Responsible for the security of the cloud
Customers own the data and are responsible for the security of their data Qubole is granted rights to process the data in the customer's account	Responsible for secure access to data platform	Responsible for secure storage in the cloud
Responsible for data encryption	Responsible for secure transport of commands	Responsible for availability and redundancy in the cloud
Responsible for user management	Responsible for multi-factor authentication for administrative access to systems with more highly sensitive and regulated data	Responsible for compute resources in the cloud
Responsible for infrastructure identity and access management	Responsible for operating system, firewall configuration	Responsible for networking in the cloud
Responsible for Qubole groups and role definitions	Responsible for metadata security	Responsible for encryption technology, key management capabilities
Responsible for data residency. Responsible for requesting and reviewing 3rd party attestation and certification reports	Responsible for 3rd party attestation/validation (SOC2, HIPAA, PCI)	Responsible for 3rd party attestation/validation (SOC2, HIPAA, PCI)

Leveraging Qubole for GDPR

Qubole provides the following functionality to assist you with data governance and security.

GDPR requires you to:	QDS allows you to:
Control Access to Personal Data A pillar of GDPR is limiting who has access to crucial data in your domain. While it sounds simple, consolidating a list of administrators is tricky. Limiting and tracking access to your applications can prove even trickier.	**Enforce a Least Privilege Model** You can restrict who can view, create, edit, and delete your most sensitive data objects using: 1. Privileges based on job requirements using Identity and Access Management (IAM) roles in AWS and other types of Role-Based Access (RBAC) in Azure and Oracle Cloud. 2. Qubole also supports Amazon AWS Key Management Service (KMS). This service stores keys in a shared Hardware Security Module (HSM) dedicated to encryption key storage. 3. Qubole provides a policy document that is GDPR compliant. This policy defines the permissions that apply to a user, group, or role; the permissions in turn determine what users can do in AWS.
Follow the Right to Be Forgotten This rule allows a person to request that any data a company owns about them be deleted. This can be anything about a specific individual, ranging from a social security number to a CRM record. While this rule cannot supersede another law (like a requirement to maintain HIPAA records), it is essential for any company who houses personal data online.	**Discover and Delete Data** Qubole has a data deletion process that allows you to comply with requests from individuals exercising their right to erasure. **Note:** This process only covers the Qubole customer data that is collected in the QDS service and not the customer-managed data within their environment. Please contact your account representative for access to Qubole's written data deletion process.
Report a Breach in 72 Hours In the case of a personal data breach, the Controller needs to notify their local Data Protection Authority figure within 72 hours after becoming aware of it. Companies should have a cross-functional incident response plan prepared that includes the Public Relations, Legal, Compliance, IT, and Security teams.	**Defined Policies and Procedures for Incident Reporting** Qubole has strictly enforced security policies that govern all aspects of our incident reporting process. Please contact your account representative for access to Qubole's written incident reporting process.