Dataclay

QUE Security, Privacy and Architecture Documentation

Published October 11, 2021

1. DATACLAY'S CORPORATE TRUST COMMITMENT

Dataclay is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters including protection of Customer Data as defined in Dataclay's QUE Terms of Service.

2. SERVICES COVERED

This documentation describes the architecture of, the security- and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to, the services provided by Dataclay that are branded as QUE ("**QUE Services**").

3. ARCHITECTURE AND DATA SEGREGATION

The QUE Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

4. CONTROL OF PROCESSING

Dataclay has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Dataclay and its sub-processors. In particular, Dataclay has entered into written agreements with its sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the technical and organizational data security measures implemented by Dataclay. The "Infrastructure and Sub-processors" documentation attached hereto describes the sub-processors material to Dataclay's provision of the QUE Services.

5. INFORMATION SECURITY REQUIREMENTS

5.1. Security Incident. Where Dataclay knows, or reasonably suspects, an accidental or unauthorized loss, destruction, acquisition, disclosure, access, manipulation, use or other form of compromise of Customer Data (a "**Security Incident**") has occurred, to the extent permitted by law, Dataclay will notify Customer's point of contact in writing (email is acceptable) promptly, and in any event within 48 hours following such discovery and reasonably cooperate with Customer in any breach investigation or remediation efforts. If Customer notifies Dataclay of a security vulnerability or incident that is identified by Customer or a third-party to Customer, Dataclay will, in good faith, address the security vulnerability or incident without undue delay regardless of severity. For the purposes of this Security, Privacy and Architecture Documentation **"Customer Data"** has the meaning set forth in the Agreement.

5.2. Industry Standards. Dataclay represents and warrants that it will implement appropriate technical and organizational security measures, based on current Industry Standards. **"Industry Standards"** means commercially reasonable security measures in all applicable equipment, software systems, services and platforms that Dataclay uses to access, process and/or store Customer Data, that are designed to ensure the security, integrity, and confidentiality of Customer Data, and to protect against any Security Incidents. Further, Dataclay represents and warrants it will comply with applicable laws and regulatory

requirements to ensure that Customer Data is not destroyed (except as expressly permitted under this Agreement), lost, altered, corrupted or otherwise impacted such that it is not readily usable by Customer in its business operations. Upon Customer's request, Customer Data will be promptly provided or otherwise made accessible to Customer by Dataclay using the Services or in an Industry Standard format specified by Dataclay.

5.3. Intrusion Detection. Dataclay, or an authorized independent third party, will monitor the QUE Services for unauthorized intrusions using network-based intrusion detection mechanisms. Dataclay may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes to prevent fraudulent authentications, and to ensure that the QUE Services function properly.

5.4. User Authentication. Access to the QUE Services requires a valid user ID and password combination, or an OAuth token, both of which are encrypted via TLS while in transmission. Following a successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

5.5. Illicit Code. Except for the functions and features expressly disclosed in Dataclay's Documentation provided or made available to Customer, Dataclay represents and warrants that to its actual or constructive knowledge after having exercised diligent efforts that the Services, deliverables and software and equipment that process, store or transmit Customer Data do not and will not contain any malicious or disabling code, including, but not limited to, viruses, malware, worms, back doors, date/time bombs, or Trojan horses ("**Unauthorized Code**"). Dataclay will establish and maintain technical and administrative safeguards reasonably designed and implemented to detect and protect against Unauthorized Code. The QUE Services do not scan for viruses that could be included in attachments or other data uploaded into the QUE Services by customers. Uploaded attachments are not executed in the QUE Services and therefore will not damage or compromise the online QUE Services by virtue of containing a virus.

5.6. Security of All Software Components. Dataclay will appropriately inventory all software components (including, but not limited to, open source software) used in the Services, software, equipment and/or deliverables, and provide such inventory to Customer upon request. Dataclay will assess whether any such software components have any security defects and/or vulnerabilities that could lead to a Security Incident. Dataclay will perform such assessment before delivery of, or providing access to, such software components to Customer and on an on-going basis thereafter during the term of the Agreement and any Orders and Statements of Work under the Agreement. Dataclay will remediate identified security defects or vulnerabilities in a timely manner. If security defects or vulnerabilities cannot be remediated in a timely manner, Dataclay will notify Customer so that an appropriate risk assessment can be conducted. Dataclay will not disclose any Customer Data in connection with any remediation efforts.

5.7. Backup. All Customer Data is backed up daily. Backup data is stored encrypted. Dataclay performs regular restore tests to ensure backup procedures are sound. Encryption of backup snapshots is done with rotating encryption keys.

5.8. Resiliency. During the term of the Agreement and all Orders and Statements of Work under the Agreement, Dataclay will maintain a disaster recovery ("**DR**") solution and related plan that is consistent with Industry Standards for the Services being provided. The DR solution will ensure identified critical capabilities are restored within a 72-hour period with no more than 48 hours of data loss in the event of a declared disaster or major system outage. Dataclay will provide agreed upon action plans to promptly address and resolve any deficiencies, concerns, or issues that may prevent the critical functionality of the Services from being recovered within 72 hours in the event of a disaster or major system outage.

6. SECURITY ASSESSMENT

6.1. Security Assessment. If Customer reasonably determines, or in good faith believes, that Dataclay's security practices and procedures do not meet Dataclay's obligations pursuant to the Agreement or this Security, Privacy and Architecture Documentation, then Customer may notify Dataclay of the deficiencies. In such event, Dataclay will without unreasonable delay (i) correct such deficiencies at its own expense and (ii) permit Customer, or its duly authorized representatives, on reasonable prior notice, to assess Dataclay's and Dataclay subcontractors' security-related activities that are relevant to the Agreement. Additionally, Dataclay will complete, in a timely and accurate manner, an information security questionnaire provided by Customer to Dataclay, on an annual basis or more frequently upon Customer's reasonable request, in order to verify Dataclay's and its subcontractors' compliance with their security-related obligations in the Agreement. ("**Security Assessment**").

6.2. Security Issues and Remediation Plan. Security issues identified by Customer during a Security Assessment will have an assigned risk rating and an agreed to timeframe to remediate. Dataclay will remediate all security issues identified within the agreed remediation timeframes and failure to comply will result in Customer having the right to terminate this Agreement without the payment of any early termination fee and with the right to a refund of any prepaid amounts for the period of time after the effective date of such termination.

7. INFORMATION SECURITY CONTROLS

Dataclay's policies for information security will be documented by Dataclay, approved by Dataclay's management, published and communicated to Dataclay's personnel. The QUE Services uses infrastructure provided by Amazon Web Services, Inc. ("AWS") to host or process Customer Data. Information about security and privacy-related audits and certifications received by AWS, including ISO 27001 certification and SOC reports, is available from the AWS Security website and the AWS Compliance website.

7.1. Asset Handling

a. Dataclay will classify Customer Data so that it is properly identified and access to Customer Data will be appropriately restricted.

b. Dataclay will maintain an acceptable use policy with restrictions on printing Customer Data and procedures for appropriately disposing of printed materials that contain Customer Data when such data is no longer needed to provide the QUE Services under the Agreement.

c. Dataclay will maintain an appropriate approval process whereby such approval is provided to personnel, contractors and agents before storing Customer Data on portable devices; remotely accessing Customer Data; or processing such data outside of Dataclay facilities (or AWS facilities). If storing Customer Data on portable devices is approved and granted, Dataclay will enforce the use of current Industry Standard encryption on the portable device. Dataclay will prohibit the enrollment of mobile devices that have been "jail broken."

7.2. Access Control.

a. Dataclay will maintain an appropriate access control policy that is designed to restrict access to Customer Data and Dataclay assets to authorized personnel, agents and contractors.

b. Dataclay will maintain and enforce a password policy that is aligned to current Industry Standards (e.g. NIST Cyber Security Framework and the Center for Internet Security). Customers accessing data with a satellite machine will be issued a token that the Customer is required to keep secure. Customers accessing data through an API will be issued a key that the Customer is required to keep secure.

c. Dataclay will restrict access to Dataclay systems involved in providing Services, to only those individuals who require such access to perform their duties using the principle of least privilege access.

d. Dataclay will provide an Industry Standards based single sign-on (SSO) capability (SAML, etc.) for Customer which will require authentication to access any Dataclay web-based application(s) provided as part of the Services, unless the requirement is explicitly waived by Customer.

7.3. Cryptography. Dataclay will maintain policies and standards regarding the use of cryptographic controls that are implemented to protect Customer Data.

7.4. Physical and Environmental Security.

a. AWS production data centers are used to host the QUE Services and have an access control system. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, two-factor access screening, including biometrics, and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

b. **Secure Disposal or Reuse of Equipment.** AWS will verify equipment containing storage media, to confirm that all Customer Data has been deleted or securely overwritten using Industry Standard processes before disposal or re-use.

7.5. Operations Security

a. **Logging and Monitoring of Events.** Dataclay will enable logging and monitoring on all operating systems, databases, applications, and security and network devices that are involved in providing Services.

b. **Protections from Malware.** Dataclay will maintain anti-malware controls that are designed to protect systems from malicious software, including malicious software that originates from public networks. Dataclay will maintain software at the then current major release for Dataclay owned anti-malware software and provide maintenance and support for new releases and versions of such software.

c. **Encryption of Data at Rest.** Dataclay will encrypt data at rest using current Industry Standard encryption solutions or will provide the capability with instructions to Customer so that Customer may enable further encryption, at Customer's discretion.

7.6. Communications Security

a. **Information Transfer and Storage.**

i. Dataclay will use current SSL encryption to encrypt Customer Data that is in transit using field level masking and is decrypted by Customer-installed client software (i.e., Templater™).

ii. Dataclay will restrict access through encryption to Customer Data stored on media that is physically transported from Dataclay facilities.

b. **Security of Network Services.** Dataclay will ensure that Industry Standard security controls and procedures for all network services and components are implemented whether such services are provided in-house or outsourced.

7.7. System Acquisition, Development and Maintenance

a. **Workstation Encryption.** Dataclay will require full hard disk encryption of all workstations and/or laptops used by personnel, contractors and agents where such personnel are accessing or processing Customer Data.

b. **Application Hardening.** Dataclay will maintain and implement secure application development policies, procedures, and standards that are aligned to Industry Standard practices. This applies to web application, mobile application, embedded software, and firmware development, as appropriate.

c. **System Hardening.** Dataclay will establish and ensure the use of standard secure configurations of operating systems. Images should represent hardened versions of the underlying operating system and the applications installed on the system.

d. **Infrastructure Vulnerability Scanning.** Dataclay will use Industry Standard and up-to-date products to scan its internal and external environment (e.g. servers, network devices, etc.) related to Services as needed. Dataclay will have a defined process to remediate findings.

7.8. Information Security Incident Management

a. Dataclay will maintain a record of Security Incidents noting the description of the Security Incident, the applicable time periods, the impact, the person reporting and to whom the Security Incident was reported, and the procedures to remediate the incident.

b. In the event of a Security Incident identified by Dataclay, Customer, or other third party, Dataclay will: (i) promptly investigate the Security Incident; (ii) promptly provide Customer with all relevant detailed information about the Security Incident; and (iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

c. Dataclay will track disclosures of Customer Data, including what type of data was disclosed, to whom, and the time of the disclosure.

8. ANALYTICS

Dataclay may track and analyze the usage of the QUE Services for purposes of security and helping Dataclay improve both the QUE Services and the user experience in using the QUE Services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality. Dataclay may share anonymous usage data with Dataclay's service providers for the purpose of helping Dataclay in such tracking, analysis, and improvements. Additionally, Dataclay may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our services.

Dataclay Infrastructure and Sub-processors

Published: October 11, 2021

Scope

This documentation lists the infrastructure environment and sub-processors material to the QUE Services in the table below. Capitalized terms used in this documentation are defined in Dataclay's Terms of Service and/or Data Processing Addendum.

The QUE Services are fully hosted on third party infrastructures, which operate as Dataclay's sub-processors.

Sub-processors Storing Customer Data

Currently, the Dataclay and third-party production systems used to provide the QUE Services are located in facilities in the United States. Customer accounts are established in one of these three regions based on where the customer subscribes to the QUE Services. Except as set forth in the "Additional Details" column in the table below, if a sub-processor is located in your region, your Customer Data for that sub-processor will be stored within your region. Otherwise, your Customer Data will be stored in the United States. You may also request to have your Customer Data hosted in a different region, which may be accommodated, subject to availability. If you have any questions about where your data is stored that this Documentation does not answer, please contact Customer Support.

In addition to the locations identified in the table below, Dataclay may store across its data storage locations identifying information about Customer's instance(s) and identifying information about Users for the purpose of operating the Services, such as facilitating the login process and the provision of customer support.

Infrastructure and Sub-processor Table				
Name of Service	**Sub-processors**	**Purpose of Processing**	**Location of Subprocessors**	**Additional Details**
QUE Services	Amazon Web Services	Third party hosting provider	• United States	
QUE Services	MongoDB	Dataclay QUE utilizes a MongoDB database which is deployed into the AWS infrastructure by way of MongoDB's platform service known as Cloud Atlas. This service provides additional layers of security beyond any base security measures that AWS . For example, Cloud Atlas allows only specific machine Ips to access any database, known as "IP Whitelisting".	• United States	

QUE Services	Auth0	End user account management platform. All user data is stored with Auth0	• United States	
QUE Services	Mailchimp	Emailing end-users notifications of alerts regarding their account information and data	• United States	
QUE Services	FastSpring	User subscription and payment information is stored securely with FastSpring. FastSpring acts as an authorized Dataclay reseller.	• United States	