Data Retention Policy

iQuda Ltd is hereinafter referred to as iQuda and "the company".

1.0 Overview

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that iQuda's guidelines on retention are consistently applied throughout the organisation.

2.0 Purpose

Some data that we use can be deleted almost immediately after use. But it is in the best interests of the company and our stakeholders to retain certain data for longer periods, for example for legal or contractual reasons.

This document defines our data retention policy. It addresses the types of data we typically process and defines how long we will it before it is removed from our systems. Our data retention policy aims to provide clear instructions to iQuda staff with regards to data retention. It also aims to provide assurance that we treat data carefully to our clients and other stakeholders.

This policy has been produced in response to the General Data Protection Regulations 2016 (the GDPR).

3.0 Scope

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location.
Note that the need to retain certain information can be mandated by local, industry regulations and will comply with the General Data Protection Regulations 2016 and the Data Protection Act 2018 and the Data Protection (Amendment) Act 2003. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

4.0 Policy

4.1 Types of Data

The General Data Protection Regulations (GDPR) place particular emphasis on protecting personal data. Personal data means information that relates to an identifiable individual. In short, if a living individual can be identified from a piece of information it is classified as personal data.

While many types of data require some degree of protection, this policy is primarily aimed at data that could cause harm if incorrectly handled, particularly personal data.

Examples of personal data include:

- Names
- Email addresses
- Home addresses
- Dates of birth
- Telephone numbers
- Biometric data
- Health data
- IP addresses
- Cookies

This is not an exhaustive list.

4.2 Reasons for Data Retention

iQuda does not wish to simply adopt a "save everything" approach. That is not practical or cost- effective and would place an excessive burden on the company to manage the constantly growing amount of data.

Some data, however, must be retained in order to protect the company's interests, preserve evidence, and generally conform to good business practices. Some reasons for data retention include:

- Litigation – taking or defending legal action
- Accident investigation
- Security incident investigation
- Regulatory requirements – also including compliance
- Intellectual property preservation

4.3 Data Duplication

It is common to see duplicated data stored across different systems in the form of backups or as application data. This policy therefore applies to all duplicate information. As a general rule, we discourage data duplication wherever possible. If data must be duplicated, all duplicates should be deleted as soon as practically possible.

4.4 Retention Requirements

This section sets guidelines for retaining the different types of company data.

- Personal customer data: Personal data will be held for as long as the individual is a customer of the company plus 6 years.
- Personal employee data: General employee data will be held for the duration of employment and then for 6 years after the last day of contractual employment.
- Service data (information produced in the course of providing a service e.g. ticket notes, purchase orders): service data will be held for as long as the individual is a customer of the company plus 6 years.
- Employee contracts will be held for 6 years after last day of contractual employment.
- Tax payments will be held for 6 years.
- Records of leave will be held for 6 years.
- Health data and criminal record data will be held for 6 years.

- Recruitment details: Interview notes of unsuccessful applicants will be held for 1 year after interview. This personal data will then be destroyed.
- Planning data: 6 years.
- Health and Safety: 6 years for records of major accidents and dangerous occurrences.
- Public data: Public data will be retained for 6 years.
- Operational data: Most company data will fall in this category. Operational data will be retained for 6 years.
- Critical data including Tax and VAT: Critical data must be retained for 6 years.
- Confidential data: Confidential data must be retained for 6 years.

4.5 Retention of Encrypted Data

If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

4.6 Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that information is deleted in a secure and efficient manner.

When the retention timeframe expires, iQuda will actively destroy the data covered by this policy. Paper records will be securely cross-shredded and disposed of in a confidential manner. Paper records should be cross-shredded using a company-supplied shredder only.

Electronic records will be securely deleted and removed from the “Recycle Bin” or “Trash” folder where deleted records are held. Every attempt will be made to delete all duplicate information simultaneously.

If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the company's management team.

iQuda specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself is Particularly forbidden, or destroying data in an attempt to cover up a violation of law or company policy.

4.7 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Recommend further reading:

- Q216 iQuda information classification and handling policy

- Q201 iQuda Information security policy
- Q217 iQuda ISMS policy
- QDBRP iQuda Data Breach Response Policy

5.0 Enforcement

This policy will be enforced by the Executive Team and Data Protection Officer. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Policy Review

This policy will be reviewed at least annually. The policy will be reviewed before this timeframe if the relevant supervisory authority releases new legislation or guidance.