

PDF Sample DATA RETENTION POLICY

PURPOSE, SCOPE AND **USERS**

This policy sets the required retention periods for specified categories of personal data and sets out the minimum standards to be applied when destroying certain information within **.....Ltd,** further: **the “Company”**.

This Policy applies to all business units, processes and systems in all countries in which **the Company** conducts business and has dealings with third parties/clients or suppliers.

This Policy applies to all directors, employees, agents, affiliates, contractors, consultants, advisors or service providers that may collect, process, or have access to all data including personal data. It is the responsibility of all the above to familiarise themselves with this Policy and its compliance.

This policy applies to all information used at **the Company’s** offices. Examples of documents include:

- Emails
- Hard copy documents
- Electronic copy documents
- Video and audio recordings
- Data generated via physical access control systems (CCTV)

1. Reference Documents

- EU GDPR 2016/679 Regulation of the European Parliament for the protection of natural persons and the processing of personal data and the free movement of such data
- Relevant U.K. national law or regulation for GDPR implementation
- Other relevant local laws and regulations
- Personal Data Protection, Disposal and Destruction Policies

2. Retention Rules

2.1. Retention General **Principle**

In the event, for any category of documents not specifically defined elsewhere in this Policy (and within the **Data Retention Schedule** and unless otherwise mandated differently by applicable law, the required retention period for such document will be deemed to be 2 Years from the date of creation of the document.

2.2. Retention General Schedule

The Managing Director defines the time for which the documents and electronic records to be retained in this **Data Retention Schedule**.

An exemption, retention periods within **Data Retention Schedule** can be prolonged in cases such as:

© **Compliant Quality Audits Ltd** : Phone: 07766 904918 Co. Reg. No.: 11021907 VAT No.: 282 0158 20

Commented [dk1]: It is highly recommended the data retention, destruction and disposal of data information is managed correctly in line with the GDPR control of Docs which this policy allows your business to implement now

Commented [dk2]: Retention is relevant to regulations. E.G. Company Law, HR Contractual Law, Financial Records, Employee current and past rights, Client and Supplier contracts, the schedule would define how long the information as accessible within the business

- Ongoing investigations from Member States authorities, if there is a chance records of personal data are needed by **the Company** to prove compliance per legal requirements; or
- Exercising legal rights in cases of law suits or a court proceeding recognized under local law.

2.3. Safeguarding of Data during Retention Period

The possibility that data media used for archiving will wear out shall be considered. If electronic storage media are chosen, any procedures and systems ensuring that the information can be accessed during the retention period - with respect to the information carrier and readability of formats shall be stored to safeguard the information against loss because of possible technological changes. The overall responsibility for the storage falls to **Managing Director**.

Commented [dk3]: Retained information always needs to be secured and the appropriate location of storage – electronic or hard copy, given due appreciation on internal servers plus hard copy storage and external servers or Cloud.

2.4. Destruction of Data

The data will be destroyed and or shredded according to the **Disposal and Destruction Policy, Breach, Enforcement and Compliance**.

The person appointed with responsibility for **Data Protection** is the **Managing Director**, who has the responsibility to ensure that each of the Company's offices complies with this Policy. It is also the responsibility of the **Managing Director** to assist **the Company** with enquiries from any local data protection or governmental authority. Any breach of this Policy must be reported immediately to the **Managing Director**. All instances of breaches of the Policy to be investigated with appropriate action.

Commented [dk4]: Destruction needs to follow company policy, and importantly needs to comply with formal legislation such as company law of retained docs prior to any destruction.

Failure to comply with this Policy may result in adverse consequences, but not limited to, loss of customer confidence, litigation and loss of competitive advantage, financial loss and damage to the Company's reputation. Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to Company premises or information, may therefore result in disciplinary proceedings or termination of their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.