Data Retention & Deletion Schedule

1. Purpose

This schedule defines the mandatory timeframes for the retention and secure disposal of data held by the company. It ensures the company remains compliant with the "Storage Limitation" principles of the UK GDPR, DUAA 2025, and China PIPL Article 19, which require that personal information be deleted once the purpose of processing has been achieved. This document serves as the operational framework for our annual "March Purge" and governs all digital and physical assets held by the company.

2. The “March Purge”

On the first Monday of March each year, the Privacy Lead (or Operative) will conduct a manual audit of all digital storage (Cloud, Local, and Encrypted Backups). Any data that has reached its "Retention Limit" as defined below must be permanently deleted using secure "shredding" software for local files and "Empty Trash" protocols for cloud storage.

3. Retentions Schedule by Data Category

Data Category	Retention Period	Trigger Event	Deletion Action
Final Audit Reports (PDF)	6 Years	Date of Delivery	Retain for professional indemnity defense
Raw Factory Photos & Video	12 Months	Project Completion	Delete to minimise risk of "Sensitive PI" exposure
Supplier Contact IDs/Passports	90 Days	Project Completion	Delete **immediately** once the identity is verified and the report is signed off
Client Contracts (MSA/SOW)	6 Years	Contract Expiry	Retain for statutory limitation period

Financial/Invoices /HMRC Data	7 Years	End of Tax Year	Retain to meet 6-year + current year tax requirements
Unconverted Leads/Quotes	2 Years	Last Interaction	Delete if the lead has not converted to a client
VPN & Security Logs	6 Months	Date of Log	Delete unless required for an active security investigation

4. The “Litigation Hold” Exception

If the company is notified of a potential legal claim, a Subject Access Request (SAR), or an HMRC/CAC investigation, the "March Purge" is suspended for all relevant files. These files must be moved to a "Legal Hold" folder and kept until the matter is formally resolved.

5. Disposal Standards

5.1 Digital Deletion (Cloud & Local)

Production Environment: Files must be deleted using a "Permanent Purge" command (bypassing the 'Recycle Bin' or 'Trash' folder). Cloud-based caches must be manually cleared.

Secure Overwriting: For data stored on local hard drives or SSDs, the company will utilise software compliant with the NIST SP 800-88 "Clear" or "Purge" standard. This ensures that data cannot be recovered via standard laboratory forensic techniques.

Cryptographic Erasure (CE): For encrypted volumes, the primary method of disposal is the destruction of the encryption key. Once the key is deleted, the data is rendered mathematically irrecoverable.

5.2 Physical Field Assets

Removable Media: SD cards, USB drives, or external SSDs used during factory visits that are retired or reach EOL (End of Life) must be physically destroyed (e.g., via specialized industrial shredding or crushing) if Cryptographic Erasure cannot be verified.

Field Notes: Any handwritten notes, factory floor sketches, or temporary printed documents must be cross-cut shredded to a minimum of DIN P-4 standard immediately after the data has been digitised and uploaded to the UK secure server.

5.3 Verification of Disposal

Deletion Certificate: Upon completion of the **March Purge**, the Privacy Lead must generate a "Record of Destruction" log. This log must record:

1. The Date of Deletion.
2. The categories of data removed.
3. The specific software/method used

Self-Audit: This log is internal and serves as the primary evidence of compliance for any future regulatory audit or client due diligence request.

Version History

Version	Date	Description of Changes
v1.0	09/03/2026	Initial Release

Next Expected Review : March 2027