Data Retention Schedule Policy for DBS e-Bulk Services

Version: 1.2

Approved by: Duncan Horsfall

1. Purpose

This document outlines the data retention schedule for Disclosure and Barring Service (DBS) applications processed through e-Bulk services by Quicker DBS Limited, acting as a registered DBS umbrella body. It should also guide client organisations using our e-Bulk platform to create their own policies, ensuring alignment with the DBS Code of Practice, the Data Protection Act 2018 (UK GDPR), and other regulatory requirements.

2. Scope

This policy applies to DBS-related records processed through our e-Bulk platform, including:

- DBS application forms
- Certificate information- Identity documentation (where applicable)
- Audit and tracking data
- Correspondence and metadata related to applications

3. Retention Schedule

Data Type	Retention Period	Justification	Secure Disposal Method
Copy of DBS Certificate /Electronic result	Max 6 months	DBS Code of Practice (para 53)	Digital deletion; paper shredding; Retention only of minimal metadata: date issued, applicant name, certificate type, purpose/role, unique reference number
Application form (Electronic, paper or scanned)	Max 6 months	Audit, error correction, disputes	Digital deletion; paper shredding; Retention only of minimal metadata: date issued, applicant name, certificate type, purpose/role, unique application number, type of documents checked
Right to Work and ID documentation	Up to 2 years, after employment	Home Office Right to Work guidance	As above
Correspondence related to applications	12–24 months	Query resolution, dispute resolution, audit trail.	As above
Metadata / logs (e-Bulk tracking)	Up to 2 years	Audit, misuse prevention	Log rotation or purge
User access logs	12–24 months	Security monitoring	System purge
Summary statistics	Indefinitely	Internal reporting	Not applicable

4. Principles of Retention

Quicker DBS and Client organisations must ensure that data accessed through the e-Bulk system is retained only as long as necessary to fulfil its original purpose. All expired data must be securely and permanently deleted.

5. Responsibilities

Client organisation DPOs: Ensure local retention and deletion practices are aligned.
System administrators: Implement appropriate technical controls for data lifecycle.
e-Bulk account users: Avoid retaining certificate information beyond the retention period.

6. Exceptions

In exceptional circumstances (e.g. safeguarding cases or legal proceedings), data may be retained longer. Such cases must be documented and reviewed regularly.

7. Review

This retention policy will be reviewed annually or in response to any legal or operational changes. Client organisations will be notified of significant amendments.

8. Related Documents

Quicker DBS Limited:

- Privacy Policy
- DBS Code of Practice
- ICO Guidelines on Data Retention
- Home Office Right to Work Guidance
- Data Protection Act 2018 (UK GDPR)