

Data Retention & Deletion Policy V2.2

EFFECTIVE FROM

2 September 2026

PROVIDER

The Data Supermarket Ltd
The Innovation Centre, Brunswick Street,
Nelson, BB9 0PQ, United Kingdom

APPLIES TO

TDS Risk

STATUS

● **In force · Version 2.2**

CORE RULE

TDS Risk does not keep Customer Personal Data simply because it may be useful later. Retention is tied to a defined purpose, documented period or customer instruction, and data is deleted, anonymised or put beyond ordinary use when that purpose ends.

ON THIS PAGE

- 1. Purpose and Status
- 2. Scope
- 3. Legal Framework and Principles
- 4. Roles and Responsibility
- 5. Customer Retention Controls
- 6. Retention Schedule
- 7. Verification Request Data
- 8. Verification Results, TDS Audit and Risk Recall
- 9. Mobile Intelligence and Identity Data
- 10. Account, Security and Operational Records
- 11. Billing, Tax and Legal Records
- 12. Backups and Disaster Recovery
- 13. How Deletion Works
- 14. Account Closure and Termination
- 15. Data Subject Rights and Erasure
- 16. Legal Holds and Exceptions
- 17. Sub-processors
- 18. Anonymisation and Aggregated Data
- 19. Changes, Logging and Governance
- 20. Contact
- Schedule 1** · Retention matrix
- Schedule 2** · Deletion states

1 Purpose and Status

1.1

This policy explains how The Data Supermarket Ltd ("TDS") sets, applies, records and enforces retention and deletion periods for Personal Data processed through TDS Risk.

1.2

It is intended to support compliance with the UK GDPR storage-limitation and accountability principles, the Data Protection Act 2018, relevant provisions of the Data (Use and Access) Act 2025, the TDS Risk Terms of Service and the TDS Risk Data Processing Agreement ("DPA").

1.3

This policy forms part of the TDS Risk Trust Centre. Where TDS processes Customer Personal Data as Processor, the DPA prevails in the event of conflict concerning Processor obligations. Where TDS acts as an independent Controller for separate purposes, the relevant TDS privacy information and applicable law govern that Processing.

1.4

Retention periods in this policy are standard or maximum periods. TDS does not treat any period as automatically lawful for every Customer use case. A shorter period, longer justified period, legal hold, Customer instruction or Service-specific rule may apply where permitted by law and the Services.

2 Scope

2.1

This policy applies to Personal Data processed in connection with TDS Risk, including data submitted to verification endpoints, verification outputs, TDS Audit records, Risk Recall evidence, Customer References, account information, security and operational logs, billing records and support records.

2.2

It applies to production systems, approved support systems, data stores, logs and backups controlled by TDS, and to relevant Sub-processors to the extent required by the DPA and applicable law.

2.3

It does not require TDS to retain data that a Service is designed not to store, and it does not authorise storage prohibited by law, carrier or data-supplier terms, or applicable security requirements.

3 Legal Framework and Principles

3.1

TDS applies the storage-limitation principle: Personal Data must be kept in identifiable form for no longer than is necessary for the purpose for which it is processed.

3.2

Retention periods are selected by reference to the purpose of Processing, Customer instructions, contractual requirements, legal or regulatory obligations, security and fraud-prevention needs, dispute and claims requirements, technical constraints and the rights and freedoms of individuals.

3.3

TDS maintains documented retention rules and reviews them when Services, law, risk or technical architecture materially change.

3.4

Expiry does not always mean the same technical action. Depending on the category, expiry results in secure deletion, irreversible anonymisation, removal of direct identifiers, tokenisation, or data being placed beyond ordinary use pending expiry of protected backup media

4 Roles and Responsibility

4.1

Where TDS processes Customer Personal Data on the Customer's documented instructions, the Customer determines the purposes of Processing and is responsible for selecting a retention period appropriate to those purposes.

4.2

TDS may determine the technical method used to implement the Customer's retention instruction, including deletion jobs, storage architecture, backup rotation and methods of secure disposal, provided that TDS remains within the Customer's documented instructions and applicable law.

4.3

Customer-configurable retention does not apply to Personal Data TDS lawfully Processes as an independent Controller for its own separate purposes, including where applicable account administration, platform security, fraud prevention, billing, legal compliance or the establishment, exercise or defence of legal claims.

IMPORTANT

A Customer setting is a documented Processing instruction. It is not a statement by TDS that the selected period is legally appropriate for the Customer's own purpose. Customers remain responsible for being able to justify the period they select.

5 Customer Retention Controls

5.1

TDS Risk provides retention controls within account settings for categories of Customer Personal Data that TDS processes on the Customer's behalf.

5.2

Customers can configure separate retention periods for:

- raw verification data; and
- TDS Audit and Risk Recall evidence.

These controls are separate because the data serves different purposes and may require different retention periods.

5.3

TDS must not offer a Customer control that permits retention of data TDS is prohibited from storing or retaining under applicable law, carrier or data-supplier terms, or the architecture of the relevant Service. Customer settings may only control categories TDS is permitted and technically designed to retain.

5.4

Before a retention change is saved, TDS explains the operational consequences of that change, including where shortening a retention period may make existing records eligible for deletion and where deletion will end the availability of Risk Recall for affected verification records.

5.5

A retention-setting change must be recorded in the TDS Risk Account Audit Log with the actor, timestamp, previous setting, new setting and effective scope.

5.6

A reduction in a retention period applies to future records by default. Where a Customer chooses to apply a shorter retention period to existing eligible records, TDS requires an explicit instruction and additional confirmation before affected records become eligible for deletion. A longer period also applies to future records by default. Where supported, extending retention to existing eligible records requires a separate Customer instruction and cannot restore data that has already been deleted or irreversibly anonymised.

5.7

TDS may impose minimum or maximum technical limits where required for security, legal compliance, product integrity or third-party obligations. Applicable minimum or maximum retention limits are communicated through the Service or relevant TDS Risk documentation.

6 Retention Schedule

6.1

Schedule 1 contains the standard retention framework for TDS Risk.

6.2

Where a Customer-configurable setting applies, the selected period is calculated from completion of the relevant verification event unless the Service expressly states otherwise. The selected period takes precedence over the standard Customer-data default, subject to mandatory minimums, maximums, legal holds, prohibited storage rules and applicable law.

6.3

TDS may apply shorter technical retention for transient data where the Service does not require persistence.

7 Verification Request Data

7.1

Verification request data may include a mobile number, name, date of birth, address, Customer Reference and other data expressly supported by the selected endpoint.

7.2

TDS minimises the persistence of raw verification request data. Raw request data is not copied into general application logs, analytics systems or other secondary stores unless required for a defined operational, security or legal purpose and subject to appropriate access and retention controls.

7.3

The standard account default for raw verification request data is **7 days**. Customers may select deletion after processing, 24 hours, 7 days, 30 days or 90 days. Raw request data is not retained for six years merely because verification evidence is retained for six years; the evidential record is designed to stand on its own with minimised identifiers.

7.4

Standard self-service options are: delete after processing; 24 hours; 7 days (default); 30 days; or 90 days. Longer raw-request retention is not a standard option. Any exception requires a documented Customer instruction, a defined purpose and TDS approval.

7.5

Deletion of raw request data does not necessarily delete the separately retained verification evidence described in section 8.

8 Verification Results, TDS Audit and Risk Recall

8.1

TDS Audit and Risk Recall are designed to preserve evidence of what verification was performed and what output was returned at a particular time.

8.2

Verification evidence may include Request ID, Customer Reference, timestamp, signature, check type, frozen output, relevant signals, lawful-basis or recognised-interest declaration where applicable, declared use case, policy/version metadata and other evidence necessary to retrieve or verify the original record.

8.3

The standard account default for verification evidence is **6 years** from completion of the verification event. Customers may select a shorter supported period. Six years is a TDS standard evidential period, not a statement that UK GDPR requires six-year retention in every case. The Customer remains responsible for selecting and being able to justify a period appropriate to its purpose.

8.4

Risk Recall remains available only while the underlying verification evidence needed for Recall remains retained. Under the standard setting, a verification remains recallable for up to 6 years unless the Customer selects a shorter period, instructs earlier deletion, or an applicable legal requirement or lawful exception changes the period.

8.5

TDS minimises the personal data contained within verification evidence. Wherever reasonably possible, TDS uses references, masked values, hashes, result codes and derived indicators rather than retaining unnecessary raw personal data.

8.6

Expired verification evidence must not remain accessible merely because the Customer's account remains open.

9 Mobile Intelligence and Identity Data

9.1

Trust Score and Mobile KYC are the core TDS Risk verification products covered by this policy. Processing may include a mobile telephone number, identity attributes supplied by the Customer, carrier-derived or telecommunications-related signals, match results, reason codes and the frozen verification output.

9.2

TDS separates short-lived raw verification data from longer-lived TDS Audit and Risk Recall evidence. This allows Customers to minimise the retention of raw personal data while preserving appropriate evidence of a verification event for the period selected by the Customer.

9.3

TDS Audit and Risk Recall evidence may include the Request ID, Customer Reference, timestamp, check type, returned result and signals, applicable reason codes, policy version and related compliance metadata, and other information necessary to evidence the verification event.

9.4

A six-year evidential period may be appropriate for customers that need to investigate historic fraud, complaints, regulatory issues, disputes or legal claims. It is not a universal legal requirement. Customers should select a shorter supported period where six-year retention is not reasonably necessary for their purpose.

9.5

Where TDS receives carrier-derived or supplier-derived signals subject to contractual retention restrictions, those restrictions take precedence over a Customer-selected longer period. TDS may retain the permitted derived result or evidential representation where contractually and legally allowed, without retaining restricted upstream raw data.

10 Account, Security and Operational Records

10.1

TDS may retain account, authentication, API-key, security, abuse-prevention, administrative-access and operational records, including the TDS Risk Account Audit Log, for separate purposes necessary to operate, evidence and protect TDS Risk.

10.2

The standard retention period for the Account Audit Log is **6 years** from the relevant event. This supports accountability, security investigation, dispute handling and evidential continuity. TDS keeps the period under review and may apply a shorter period where the record is no longer necessary, or a longer period where a specific lawful requirement or legal hold applies.

10.3

The Account Audit Log records material events affecting the TDS Risk account, including relevant authentication and security events, user and permission changes, API key activity, privacy and policy monitoring events, Risk Recall activity, material account-setting changes, administrative access, retention and deletion events, webhook configuration events and other security or compliance events supported by the service.

TDS minimises personal data within the Account Audit Log and, where appropriate, records identifiers, references and event metadata rather than unnecessary raw personal data.

10.4

Other operational and security logs may have shorter documented retention periods according to security need, volume, risk and incident-investigation requirements. The six-year Account Audit Log period does not mean all low-level infrastructure logs are retained for six years.

11 Billing, Tax and Legal Records

11.1

Billing, invoice, payment, accounting and tax records may be retained separately from verification data for periods required by UK law and legitimate business administration.

11.2

Where relevant, TDS retains VAT and associated business records for the period required by applicable tax law. UK VAT records are generally required to be kept for at least six years, with longer or different periods applying in some circumstances or schemes.

11.3

Records reasonably required for a dispute, complaint, regulatory enquiry, litigation, legal claim or enforcement matter may be retained for the duration reasonably necessary to establish, exercise or defend legal rights, subject to appropriate access restrictions.

11.4

A Customer cannot use the verification retention setting to require deletion of a record that TDS is legally required or independently entitled to retain for a separate lawful purpose.

12 Backups and Disaster Recovery

12.1

Production deletion may not immediately remove every residual copy from encrypted backups or disaster-recovery media.

12.2

Where immediate selective deletion from a backup is not technically practicable, expired Personal Data must be put beyond ordinary use, protected by appropriate security controls and allowed to expire through the documented backup rotation process. Backup data subject to deletion must not be used for any other purpose.

12.3

TDS must not restore expired Personal Data into ordinary production use. If a backup restoration temporarily reintroduces expired data, the relevant deletion process must be reapplied as soon as reasonably practicable.

12.4

Backup retention is controlled separately by TDS and does not extend the applicable retention period for active production data. Where TDS is legally required to retain information beyond its normal period, access remains restricted and the information is retained only for as long as that requirement applies.

13 How Deletion Works

13.1

At the end of the applicable retention period, eligible data is queued for the action defined by the relevant retention rule.

13.2

TDS operates deletion processes to identify records that have reached the end of their applicable retention period and make them eligible for deletion or anonymisation in accordance with this policy.

13.3

Where deletion is subject to a short processing window for system integrity, queues or distributed storage, the data must no longer be available for ordinary Customer use after expiry and must be physically deleted or irreversibly anonymised as soon as reasonably practicable.

13.4

TDS records non-content metadata relating to material deletion activity in the Account Audit Log or other appropriate audit records. This may include the deletion job reference, affected data category, number of records processed, timestamp, outcome and actor or system responsible for initiating the action.

13.5

Deleted Personal Data is not reconstructed from ordinary TDS production systems. Residual protected backup copies are handled in accordance with section 12.

14 Account Closure and Termination

14.1

Closing a TDS Risk account does not automatically require immediate destruction of every category of data. The applicable DPA, Customer instructions, legal obligations, security requirements and this policy determine what happens to each category.

14.2

For Customer Personal Data processed solely as Processor, TDS shall delete or return the data at the Customer's choice at the end of the relevant Processing, subject to the DPA and applicable law.

14.3

Customer-facing access may be disabled before backend deletion is complete.

14.4

TDS may retain data it lawfully Processes as independent Controller, or data subject to a legal hold, for the applicable separate period.

15 Data Subject Rights and Erasure

15.1

Retention settings do not remove or restrict applicable data-subject rights.

15.2

Where TDS acts solely as Processor for Customer Personal Data, TDS will assist the Customer with erasure and other rights requests in accordance with the DPA.

15.3

A valid erasure instruction may require deletion before the scheduled retention date. Conversely, a right-to-erasure request is not absolute and does not require deletion where an applicable legal exception permits or requires continued Processing.

15.4

Where TDS acts as independent Controller for the relevant data, requests are handled under the TDS Privacy Policy and applicable law.

16 Legal Holds and Exceptions

16.1

TDS may suspend scheduled deletion of specific records where retention is reasonably necessary and lawful for litigation, anticipated litigation, a regulatory or law-enforcement request, investigation, fraud or abuse investigation, legal obligation, dispute or the establishment, exercise or defence of legal claims.

16.2

Information subject to a legal hold is restricted to the purpose for which the hold applies and is not retained indefinitely by default.

16.3

TDS reviews the continued need for a legal hold. When the hold ends, the information returns to the applicable retention and deletion process, and any information that has already exceeded its applicable retention period is deleted without undue delay unless another lawful basis requires continued retention.

17 Sub-processors

17.1

TDS requires relevant Sub-processors to protect Customer Personal Data and to support deletion or return obligations to the extent required by applicable Data Protection Law and the DPA.

17.2

TDS remains responsible for ensuring that its own retention commitments are capable of being implemented through relevant Sub-processor arrangements.

17.3

Where Sub-processor backup cycles affect deletion timing, TDS requires residual copies to remain appropriately safeguarded and to expire in accordance with the applicable contractual and legal framework.

18 Anonymisation and Aggregated Data

18.1

TDS may irreversibly anonymise data instead of deleting it where the resulting information no longer constitutes Personal Data and the method used is reasonably designed to prevent re-identification.

18.2

Merely removing a name or replacing an identifier with a reversible token does not, by itself, make data anonymous.

18.3

Truly anonymous statistical information may be retained for analytics, security, capacity planning, product performance or service-improvement purposes because it is no longer Personal Data.

18.4

TDS must not describe pseudonymised or tokenised data as anonymous where TDS or another party can reasonably re-identify the individual using additional information.

19 Changes, Logging and Governance

19.1

TDS maintains version and effective-date information for this policy.

19.2

TDS maintains appropriate technical and organisational measures to support the retention periods and deletion processes described in this policy.

19.3

Access to retention controls and deletion functionality is restricted to appropriately authorised users. Material changes to retention settings and deletion activity are recorded for audit purposes.

19.4

TDS monitors the operation of its retention and deletion controls and investigates identified failures or exceptions in accordance with its security, incident-management and governance procedures.

19.5

TDS reviews this policy at least annually and sooner where there is a material change to TDS Risk, applicable law, carrier or data-supplier requirements, or retention architecture.

20 Contact

20.1

Customers may contact TDS through the contact details published in the TDS Risk Trust Centre for questions about retention, deletion, data-subject requests or the operation of account retention controls.

20.2

Customers requiring a bespoke retention arrangement should contact TDS before relying on a period that is not available through the standard Service controls.

Retention Matrix

The matrix below sets out the standard retention framework for TDS Risk. The period applicable to a particular record may vary where a Customer selects a permitted alternative retention period, a legal hold applies, a legal or regulatory requirement requires continued retention, or a service-specific restriction applies

CATEGORY	ROLE	DEFAULT	CUSTOMER CONTROL	OPTIONS / RULE	END ACTION
Verification request data	Processor	7 days	Yes	After processing / 24h / 7d / 30d / 90d	Secure deletion; longer period only by documented justified arrangement
Verification outputs + TDS Audit + Risk Recall evidence	Processor	6 years	Yes	6 years default; shorter Customer-selected periods supported	Delete or irreversibly anonymise; Risk Recall ends
Customer Reference / linkage metadata	Processor	Same as associated verification evidence (6 years default)	Indirect	Follows evidence setting	Delete with associated evidence unless independently required
Account / profile data	Controller and/or Processor depending on activity	While account is active + applicable closure period	No	TDS-controlled	Delete / anonymise subject to legal and security needs
Account Audit Log	TDS Controller and/or Processor depending on event	6 years	No	TDS standard evidential period; reviewed for necessity	Delete / anonymise after retention period unless hold applies
Billing / tax / accounting records	TDS Controller	At least 6 years where VAT law requires; longer where applicable	No	TDS-controlled	Delete after statutory / business need ends
Support records	Depends on context	Purpose-based	No general control	TDS-controlled or case-specific	Delete when support / legal purpose ends
Backups	Mirrors source role	Backup rotation period	No	TDS-controlled	Beyond ordinary use, then expiry through rotation
Legal-hold records	Depends on underlying role	Duration of hold	No	Hold overrides scheduled deletion	Delete when hold ends unless another lawful need remains

Deletion States

Active	Within applicable retention period and available to authorised systems / users.
Expiry Due	Retention period reached; record no longer required for ordinary use and queued for deletion / anonymisation.
Deletion pending	Awaiting completion of deletion across active stores or dependent systems; customer access removed where applicable.
Deleted	Active copy securely deleted and not recoverable from ordinary TDS systems.
Anonymised	Direct and indirect identifiers removed or transformed so the information is no longer Personal Data.
Backup only	Residual protected copy may exist only within backup rotation; not available for ordinary use and must not be restored into ordinary processing without reapplying deletion.
Legal hold	Scheduled deletion temporarily suspended for a specific lawful reason; access restricted and hold reviewed.