

Data Processing Agreement V1.1

EFFECTIVE FROM

1 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 1.1**

ON THIS PAGE

- 1. Scope and Application
- 2. Definitions
- 3. Roles of the Parties
- 4. Processing Details
- 5. Documented Instructions
- 6. Confidentiality
- 7. Security of Processing
- 8. Sub-processors
- 9. Data Subject Rights
- 10. Assistance to the Customer
- 11. Personal Data Breaches
- 12. Return and Deletion
- 13. Audits and Compliance Information
- 14. International Transfers
- 15. Records and Regulatory Cooperation
- 16. Customer Responsibilities
- 17. Liability and Relationship with the Terms
- 18. Changes to this DPA
- 19. Acceptance and Effect
- Schedule 1** · Details of Processing
- Schedule 2** · Technical and Organisational Measures
- Schedule 3** · Sub-processors

1 Scope and Application

1.1

This Data Processing Agreement ("DPA") forms part of the agreement between The Data Supermarket Ltd ("TDS") and the customer using TDS Risk ("Customer").

1.2

This DPA applies to the extent that TDS processes Personal Data on behalf of the Customer as a Processor in connection with TDS Risk.

1.3

This DPA is incorporated into the TDS Risk Terms of Service. In the event of a conflict between this DPA and the Terms concerning the Processing of Customer Personal Data, this DPA shall prevail to the extent of that conflict.

1.4

This DPA does not apply to Processing for which TDS acts as an independent Controller.

1.5

Where TDS Processes Personal Data for its own separate and lawful purposes, including where applicable service administration, security, fraud prevention, billing, legal or regulatory compliance, or the establishment, exercise or defence of legal claims, such Processing shall be governed by applicable Data Protection Law and the relevant TDS privacy information.

2 Definitions

2.1

In this DPA:

“Controller”, “Processor”, “Personal Data”, “Personal Data Breach”, “Processing”, “Process”, “Data Subject” and “Supervisory Authority” have the meanings given under applicable Data Protection Law.

“Customer Personal Data”

means Personal Data Processed by TDS on behalf of the Customer in connection with the Services.

“Data Protection Law”

means applicable UK legislation relating to privacy and the Processing of Personal Data, including the UK GDPR, Data Protection Act 2018 and relevant provisions of the Data (Use and Access) Act 2025, in each case as amended, replaced or supplemented from time to time.

“Services”

means the applicable TDS Risk products, APIs, platform functionality and associated services used by the Customer.

“Sub-processor”

means another Processor engaged by TDS to Process Customer Personal Data on behalf of the Customer.

“Terms”

means the applicable TDS Risk Terms of Service.

2.2

Capitalised terms not defined in this DPA have the meanings given in the Terms.

3 Roles of the Parties

3.1

Where TDS Processes Customer Personal Data on the documented instructions of the Customer:

Customer	Controller
TDS	Processor

3.2

The allocation in clause 3.1 applies on a Processing-activity basis.

3.3

Either party may separately act as an independent Controller for Personal Data it Processes for its own purposes.

3.4

Nothing in this DPA determines the legal status of either party contrary to the factual circumstances of the relevant Processing.

4 Processing Details

4.1

The subject matter, nature, purpose and duration of Processing, together with the categories of Personal Data and Data Subjects, are described in [Schedule 1 – Details of Processing](#).

4.2

The Customer determines the purposes for which Customer Personal Data is submitted to TDS Risk and whether use of the Services is appropriate for those purposes.

5 Documented Instructions

5.1

TDS shall Process Customer Personal Data only on documented instructions from the Customer unless Processing is required by applicable UK law.

5.2

Documented instructions may include:

- the TDS Risk Terms of Service;
- this DPA;
- API requests;
- API-key configuration;
- service selections;
- lawful-basis declarations;
- recognised-interest declarations where applicable;
- declared use cases;
- settings selected through the TDS Risk platform;
- support instructions; and
- other written instructions accepted by TDS.

5.3

Where applicable law requires TDS to Process Customer Personal Data other than on the Customer's instructions, TDS shall notify the Customer before Processing unless applicable law prohibits that notification.

5.4

If TDS reasonably believes an instruction infringes applicable Data Protection Law, TDS shall inform the Customer and may suspend the affected Processing pending clarification or amendment of the instruction.

6 Confidentiality

6.1

TDS shall ensure that persons authorised to Process Customer Personal Data:

- are subject to appropriate contractual or statutory confidentiality obligations;
- receive access only where reasonably necessary for their authorised functions; and
- Process Customer Personal Data only as authorised.

6.2

TDS shall take reasonable steps to ensure that access to Customer Personal Data is limited to personnel and systems requiring access for the provision, support, security or administration of the Services

7 Security of Processing

7.1

Taking into account the state of the art, costs of implementation, nature, scope, context and purposes of Processing and the risks to individuals, TDS shall implement and maintain appropriate technical and organisational measures designed to protect Customer Personal Data.

7.2

Such measures shall be designed, as appropriate, to protect against:

- accidental or unlawful destruction;
- loss;
- alteration;
- unauthorised disclosure;
- unauthorised access; and
- other unlawful Processing.

7.3

The categories of technical and organisational measures maintained by TDS are described in [Schedule 2 – Technical and Organisational Measures](#).

7.4

TDS may modify individual security technologies, suppliers, configurations or implementations from time to time, provided that TDS does not materially reduce the overall level of protection applicable to Customer Personal Data.

8 Sub-processors

8.1

The Customer grants TDS general written authorisation to engage Sub-processors to Process Customer Personal Data where reasonably necessary to provide, operate, secure or support the Services.

8.2

TDS maintains a current Sub-processor Register within the TDS Risk Trust Centre.

8.3

The current Sub-processor Register is incorporated into this DPA by reference.

8.4

Before permitting a Sub-processor to Process Customer Personal Data on behalf of the Customer, TDS shall impose written data-protection obligations providing a level of protection materially equivalent to the applicable obligations imposed on TDS under this DPA, to the extent required by applicable Data Protection Law.

8.5

TDS shall remain responsible for the performance of its Sub-processors to the extent required by applicable Data Protection Law.

8.6

The appointment, replacement, notification and objection arrangements applicable to Sub-processors are set out in **Schedule 3 – Sub-processors**.

9 Data Subject Rights

9.1

Taking into account the nature of the Processing, TDS shall provide reasonable assistance to the Customer through appropriate technical and organisational measures, insofar as reasonably possible, to enable the Customer to respond to requests by Data Subjects exercising their rights under applicable Data Protection Law.

9.2

Where TDS receives a request directly from a Data Subject concerning Customer Personal Data for which TDS acts solely as Processor, TDS shall notify or refer the request to the Customer as appropriate, unless applicable law prohibits TDS from doing so or requires TDS to respond directly.

9.3

TDS shall not independently respond to such a request on behalf of the Customer except:

- on documented Customer instructions; or
- where required by applicable law.

10 Assistance to the Customer

10.1

Taking into account the nature of the Processing and information available to TDS, TDS shall provide reasonable assistance to the Customer with applicable obligations relating to:

- security of Processing;
- Personal Data Breaches;
- Data Protection Impact Assessments;
- prior consultation with a Supervisory Authority where required;
- Data Subject rights; and
- other matters for which Processor assistance is required by applicable Data Protection Law.

11 Personal Data Breaches

11.1

TDS shall notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data Processed by TDS as Processor.

11.2

Where reasonably available, TDS shall provide information

concerning: • the nature of the Personal Data Breach;

- categories of affected Personal Data;
- categories and approximate number of affected Data Subjects where known;
- approximate number of affected Personal Data records where known;
- likely consequences where known;
- measures taken or proposed to address the breach;
- measures intended to mitigate possible adverse effects where appropriate; and
- other information reasonably required by the Customer to meet applicable legal obligations.

11.3

Where all information is not immediately available, TDS may provide it in stages without undue further delay.

11.4

Notification of a Personal Data Breach does not constitute an acknowledgement by TDS of fault or liability.

12 Return and Deletion

12.1

Following termination of the relevant Processing, TDS shall, at the Customer's choice and subject to applicable law:

- delete Customer Personal Data Processed solely on behalf of the Customer; or
- return such Customer Personal Data to the Customer and delete remaining copies.

12.2

Clause 12.1 does not require deletion of Personal Data:

- which applicable UK law requires TDS to retain;
 - which TDS lawfully Processes as an independent Controller;
 - which is reasonably required for the establishment, exercise or defence of legal claims;
- or • which may otherwise lawfully be retained under applicable Data Protection Law.

12.3

Any Customer Personal Data retained under clause 12.2 shall remain subject to applicable confidentiality and security obligations for as long as it remains Personal Data.

12.4

Customer Personal Data may be deleted automatically in accordance with the applicable Services, the Terms, documented retention periods, Customer instructions and applicable law.

13 Audits and Compliance Information

13.1

TDS shall make available to the Customer information reasonably necessary to demonstrate compliance with the Processor obligations applicable to TDS under this DPA and applicable Data Protection Law.

13.2

TDS shall allow for and contribute to audits and inspections to the extent required by applicable Data Protection Law.

13.3

Where appropriate, TDS may initially satisfy a reasonable audit request by providing:

- security documentation;
- completed security questionnaires;
- compliance reports;
- independent assurance or penetration-test summaries;
- certifications;
- policies;
- technical documentation; or
- written responses.

13.4

Where additional inspection is reasonably required, the parties may agree appropriate arrangements concerning:

- reasonable notice;
- scope;
- frequency;
- timing;
- confidentiality;
- security restrictions;
- personnel;
- method; and
- reasonable costs,

provided those arrangements do not prevent the Customer exercising a mandatory statutory right.

13.5

Audits shall not require TDS to disclose information which would:

- compromise another customer's confidentiality or security;
- expose credentials, keys or exploitable security information;
- breach applicable law or third-party confidentiality obligations; or

- materially compromise TDS systems,

provided TDS supplies reasonable alternative evidence where necessary to meet its legal obligations.

14 International Transfers

14.1

TDS shall ensure that any restricted transfer of Customer Personal Data outside the United Kingdom by TDS, or by an authorised Sub-processor in connection with the Services, is carried out in accordance with applicable Data Protection Law.

14.2

Where a restricted transfer requires an international data-transfer mechanism or safeguard, TDS shall ensure an appropriate lawful mechanism is in place.

14.3

Such mechanisms may include, where applicable:

- UK adequacy regulations;
- the UK International Data Transfer Agreement;
- the UK Addendum to the EU Standard Contractual Clauses; or
- another lawful mechanism recognised under applicable Data Protection Law.

14.4

Relevant international Processing locations shall be identified through the TDS Risk Sub-processor Register where applicable.

15 Records and Regulatory Cooperation

15.1

TDS shall maintain records of Processing activities where required by applicable Data Protection Law.

15.2

TDS shall cooperate with the Information Commissioner's Office or another competent Supervisory Authority to the extent required by applicable law in relation to Processing for which TDS acts as Processor.

16 Customer Responsibilities

16.1

The Customer remains responsible for:

- identifying an appropriate lawful basis for its Processing;
- determining whether TDS Risk is appropriate for the intended purpose;
- providing all required privacy information;
- ensuring Personal Data submitted to TDS is adequate, relevant and limited to what is necessary;
- ensuring it has authority to instruct TDS to Process that information;
- ensuring its instructions comply with applicable law;

- responding to applicable Data Subject rights;
- determining appropriate retention periods within its own systems;
- maintaining appropriate technical and organisational security;
- maintaining appropriate human and/or automated decision-making practices; and
- ensuring use of TDS Risk results complies with applicable law.

16.2

TDS Risk provides signals, intelligence and verification outputs. Unless expressly agreed otherwise, TDS does not determine the Customer's final eligibility, fraud, credit, insurance, claims, onboarding or other business decisions.

17 Liability and Relationship with the Terms

17.1

Liability arising under this DPA is subject to the exclusions, limitations and allocation of liability contained in the TDS Risk Terms of Service, except to the extent such limitation is prohibited by applicable law.

17.2

Nothing in this DPA excludes or limits a Data Subject's rights or either party's liability where such exclusion or limitation is prohibited by applicable Data Protection Law.

18 Changes to this DPA

18.1

TDS may update this DPA where reasonably necessary to:

- reflect changes in Data Protection Law;
- reflect regulatory guidance;
- improve the protection of Personal Data;
- reflect changes to the Services or Processing; or
- address changes to approved transfer mechanisms or Sub-processors.

18.2

Material changes shall be notified or made available to Customers in accordance with the TDS Risk Terms of Service.

18.3

TDS shall maintain version and effective-date information for this DPA.

19 Acceptance and Effect

19.1

This DPA becomes binding between TDS and the Customer when the Customer:

- accepts or enters into the TDS Risk Terms of Service which incorporate this DPA;
- enters into an Order Form, agreement or other written arrangement incorporating this DPA; or

- otherwise expressly agrees to this DPA.

19.2

A separate signature is not required where this DPA has been validly incorporated into a binding agreement between TDS and the Customer.

19.3

Where the parties execute a separately signed version of this DPA, that signed version shall apply subject to any agreed amendments expressly recorded in writing.

SCHEDULE 1

Details of Processing

1. SUBJECT MATTER	Provision of TDS Risk fraud, mobile intelligence, identity verification, auditing, monitoring and associated Services selected by the Customer.
2. DURATION	Processing continues for: • the period during which TDS provides the relevant Service; and • any subsequent period during which Processing or retention is required by the Customer's documented instructions or applicable law. Any separate Processing undertaken by TDS as an independent Controller is outside the scope of this Schedule and is addressed under clauses 1.4, 1.5 and 12.2 of this DPA.
3. NATURE OF PROCESSING	Depending upon the Services used, Processing may include: • receipt; collection; transmission; querying; comparison; verification; analysis; retrieval; • temporary or persistent storage; generation and transmission of verification outputs; • audit logging; security monitoring; support; deletion; and • other Processing reasonably necessary to provide the selected Services.
4. PURPOSE	To provide the TDS Risk Services selected by the Customer, including fraud and mobile intelligence, identity verification and associated audit, security and compliance functionality.
5. CATEGORIES OF PERSONAL DATA	Depending upon the Service used, Customer Personal Data may include: • mobile telephone number; name; date of birth; address; Customer Reference; • telecommunications-related signals; mobile-network signals; fraud or risk signals; • verification outputs; account identifiers; transaction or event references; technical or security information; and

- other Personal Data expressly submitted through an approved TDS Risk endpoint.

6. CATEGORIES OF DATA SUBJECT	May include: • customers; prospective customers; applicants; claimants; account holders; • leads; users; authorised representatives; persons involved in transactions; and • other individuals legitimately submitted by the Customer for an approved purpose.
--------------------------------------	---

7. FREQUENCY	Processing occurs on an event-driven basis when initiated or configured by the Customer through the TDS Risk platform, API or other approved Service functionality.
---------------------	--

8. RETENTION	Customer Personal Data is retained in accordance with: • the applicable Service configuration; • the Terms; • documented TDS retention periods; • Customer instructions; and • applicable legal requirements. Specific retention information may be set out in the applicable TDS Risk Data Retention & Deletion Policy.
---------------------	--

SCHEDULE 2

Technical and Organisational Measures

TDS maintains technical and organisational measures appropriate to the nature of the Services, the relevant Processing and the risks to the rights and freedoms of individuals. Depending on the nature of the Service and Processing, these measures include, where applicable:

1 Access Control restricted

- production access individual
- privileged identities
- role-based and/or least-privilege access controls
- authentication controls
- management of privileged access
- revocation of access when no longer required

2 Network and Infrastructure Security logically

- controlled cloud infrastructure network segmentation
- and access restrictions
- firewall and web-application security controls
- controlled ingress and egress
- load-balancing and application-layer protections controls
- designed to restrict unauthorised access to production workloads

3 Encryption and Credential Protection

- encryption of Personal Data in transit using appropriate transport security
- encryption at rest where appropriate to the Processing and storage technology
- controlled management of cryptographic keys secure
- storage and handling of credentials and secrets
- restrictions on access to security credentials
-

4 Application and API Security

- authenticated access to protected APIs API
- credential management
- server-side authorisation
- input validation
- abuse and rate-control measures where appropriate
- logical customer segregation
- controls designed to prevent unauthorised cross- customer access
-

5 Logging, Monitoring and Threat Detection

- security-relevant logging
- infrastructure and application monitoring
- threat-detection controls
- monitoring of privileged activity where appropriate alerting and escalation processes
- audit functionality supporting investigation of security-relevant events

6 Vulnerability and Change Management

- security-conscious development practices controlled
- production changes
- vulnerability identification and remediation
- dependency and software maintenance
- security testing appropriate to the relevant systems and risks
- penetration testing or independent security assessment where appropriate to risk

7 Resilience and Recovery

- backup procedures recovery
- procedures service monitoring
- incident-management processes
- business-continuity and disaster-recovery measures
- appropriate to the Services

8 Organisational Controls

- confidentiality obligations
- authorised-personnel restrictions
- assigned security and data-protection responsibilities
- incident-response procedures
- supplier and security due diligence where appropriate
- documented security and privacy policies
-

9 Review and Evolution

9.1

TDS reviews and evolves its technical and organisational measures having regard to changes in the Services, technology, threats and risks.

9.2

TDS may replace or modify individual technologies, suppliers, configurations or implementations as its systems evolve, provided that the overall level of protection applicable to Customer Personal Data is not materially reduced.

Sub-processor

1. General Authorisation

1.1

The Customer grants TDS general written authorisation to engage Sub-processors to Process Customer Personal Data where reasonably necessary to provide, operate, secure or support the TDS Risk Services, subject to the requirements of this DPA.

1.2

TDS shall only permit a Sub-processor to Process Customer Personal Data where that Sub-processor has been appointed in accordance with applicable Data Protection Law and this Schedule.

2. Sub-processor Register

2.1

TDS maintains a current Sub-processor Register within the TDS Risk Trust Centre.

2.2

The Sub-processor Register identifies, as applicable:

- the legal entity or service provider;
- the service or Processing purpose;
- the relevant Processing location or region; and
- the date from which the Sub-processor commenced Processing.

2.3

The current Sub-processor Register is incorporated into this DPA by reference and may be updated from time to time in accordance with this Schedule.

2.4

TDS shall take reasonable steps to keep the Sub-processor Register accurate and current.

3. Sub-processor Obligations

3.1

Before permitting a Sub-processor to Process Customer Personal Data on behalf of the Customer, TDS shall enter into a written agreement with that Sub-processor containing data-protection obligations which provide a level of protection materially equivalent to the applicable obligations imposed on TDS under this DPA, to the extent required by applicable Data Protection Law.

3.2

TDS shall take reasonable steps to assess the data-protection and security arrangements of relevant Sub-processors before appointment and thereafter as appropriate, having regard to the nature and risk of the Processing.

3.3

TDS shall remain responsible for the performance of its Sub-processors to the extent required by applicable Data Protection Law.

4. Addition or Replacement of Sub-processors

4.1

TDS shall provide the Customer, or its nominated data-protection contact where applicable, with at least 30 days' prior notice before an intended new or replacement Sub-processor begins Processing Customer Personal Data.

4.2

Notice may be provided by email, through the TDS Risk platform, through the TDS Risk Trust Centre notification mechanism, or by another reasonable electronic method.

4.3

The notice shall contain sufficient information to enable the Customer to understand the identity of the proposed Sub-processor and the nature of the Processing it is expected to perform.

5. Customer Objections

5.1

During the notice period in clause 4.1, the Customer may object to the proposed appointment on reasonable grounds relating to the protection of Customer Personal Data.

5.2

Any objection must be made in writing and provide sufficient information for TDS to understand the Customer's data-protection concerns.

5.3

Where the Customer raises a valid objection, TDS and the Customer shall work in good faith to seek a commercially reasonable solution.

5.4

A solution may include:

- implementing reasonable additional safeguards;
- using an alternative Sub-processor where reasonably available;
- modifying the affected Processing where reasonably practicable; or
- discontinuing the affected Service.

5.5

Where TDS cannot reasonably resolve a valid objection without materially affecting provision of the affected Service, the Customer may discontinue the affected Service in accordance with the TDS Risk Terms of Service.

6. International Processing

6.1

Where a Sub-processor Processes Customer Personal Data outside the United Kingdom, TDS shall ensure that any restricted transfer is carried out in accordance with applicable Data Protection Law.

6.2

Where required, TDS shall ensure that an appropriate transfer mechanism or safeguard is in place, which may include:

- UK adequacy regulations;
- the UK International Data Transfer Agreement;
- the UK Addendum to the EU Standard Contractual Clauses; or
- another lawful transfer mechanism recognised under applicable Data Protection Law.

6.3

Relevant Processing locations or regions shall be identified through the TDS Risk Sub-processor Register where applicable.

7. Changes That Do Not Constitute a New Sub-processor

7.1

TDS may update information within the Sub-processor Register without triggering the 30-day notification period where the change does not involve the appointment or replacement of a Sub-processor Processing Customer Personal Data.

7.2

This may include corrections, corporate-name changes, updated descriptions or other administrative changes which do not materially alter the relevant Processing.

8. Availability

8.1

The current Sub-processor Register shall be made available through the TDS Risk Trust Centre.

8.2

Customers may contact TDS for additional information reasonably required for their data-protection due diligence, subject to appropriate confidentiality and security restrictions.