Data Sourcing Guide

Building Trust Through Responsible Identity Intelligence

Table of Contents

Introduction

The quality, reliability and legitimacy of any data-driven service depends upon the integrity of its underlying data sources. For organisations operating in regulated industries, understanding where data originates, how it is obtained and what controls govern its use has become a critical component of our supplier due diligence.

Increasing regulatory scrutiny, evolving privacy legislation and growing public expectations around ethical data use mean organisations can no longer rely solely on contractual assurances. Procurement teams, compliance functions, privacy professionals and regulators increasingly expect evidence that data has been sourced responsibly and can withstand regulatory and reputational scrutiny.

At 1datapipe, we recognise that trust begins long before data is delivered to a customer. It begins with how data is acquired, assessed, governed and maintained throughout its lifecycle.

This guide outlines the principles, controls and governance processes that support our approach to data sourcing, quality management and ethical acquisition.

Our Philosophy

Identity intelligence can only create value when organisations have confidence in the underlying information.

Our approach is therefore built around four core principles:

- Legality
- Traceability
- Quality
- Accountability

These principles guide supplier selection, onboarding decisions, governance reviews and ongoing monitoring activities.

We believe organisations should be able to understand not only what information they are using, but also where it originated, how it was obtained and what safeguards exist to support its lawful and responsible use.

Understanding Identity Infrastructure

1datapipe operates as an identity intelligence and identity infrastructure provider.

This distinction is important.

Traditional perceptions of the data industry often focus on large-scale data aggregation without sufficient attention to governance, transparency or accountability. Modern enterprise organisations require something fundamentally different.

Identity infrastructure supports organisations in:

- Verifying identities
- Detecting fraud
- Supporting onboarding decisions
- Strengthening compliance controls

- Enhancing risk management processes
- Improving operational efficiency

The objective is not simply to provide data. The objective is to provide reliable identity intelligence supported by governance, compliance and accountability.

Data Source Categories

To support enterprise customers operating across multiple jurisdictions, data may originate from a variety of legally permissible sources.

These can include:

Government and Public Authority Records

Certain jurisdictions make specific records available through lawful mechanisms.

These records may support identity verification, validation and fraud prevention activities.

Availability varies significantly between countries and is always assessed against local legal requirements.

These authoritative government sources include national population registries and are lawfully obtained directly or through authorised intermediaries.

Telecommunications Data

Mobile Network Operators make telco-grade reference data available which is leveraged for identity corroboration and profile completeness.

Authorised Data Partners

In many jurisdictions, specialist partners provide access to locally sourced datasets and intelligence.

These relationships are governed through due diligence, contractual controls and ongoing monitoring.

Supplier Due Diligence Framework

Not all data sources meet the standards required by enterprise organisations.

For this reason, supplier onboarding is governed through a structured due diligence framework.

Assessments typically consider:

Legal Authority

Can the supplier demonstrate a lawful basis for collecting, maintaining and sharing the information?

The ability to evidence lawful collection and processing is a fundamental requirement.

Privacy Governance

Suppliers are assessed to understand their privacy frameworks, governance structures and approach to regulatory compliance.

This includes consideration of:

- Privacy notices

- Data subject rights processes
- Regulatory obligations
- Governance arrangements

Security Controls

Information security forms a critical component of supplier evaluation.

Suppliers may be assessed against factors such as:

- Access management
- Encryption
- Security governance
- Incident management
- Security assurance activities

Data Quality Processes

Data is only valuable when it is reliable.

Supplier assessments therefore consider:

- Validation processes
- Refresh schedules
- Quality controls
- Error management procedures

Contractual Commitments

Contracts help establish accountability and define expectations relating to:

- Data use
- Compliance obligations
- Security requirements
- Audit rights
- Ongoing assurance

Ethical Data Acquisition

Legal compliance alone does not automatically make data use ethical.

Enterprise organisations increasingly recognise that ethical considerations play an important role in maintaining trust and protecting reputation.

Our approach seeks to ensure that data acquisition is not only lawful but also responsible.

This includes consideration of:

- Reasonable expectations of individuals
- Transparency requirements
- Proportionality
- Privacy impact
- Risk of harm

- Governance safeguards

Ethical data acquisition requires organisations to look beyond minimum legal requirements and consider the broader implications of data use.

What We Do Not Support

Understanding what an organisation does not do can be just as important as understanding what it does.

1datapipe does not knowingly support:

- Unlawfully obtained information
- Unverifiable data sources
- Anonymous sourcing practices lacking accountability
- Data sources that cannot demonstrate legal authority
- Processing models that conflict with applicable legal requirements

These principles help reduce risk and support customer confidence.

Data Quality Framework

Enterprise decisions depend upon data quality.

Poor quality information can lead to:

- Increased fraud risk
- Operational inefficiencies
- Customer friction
- Regulatory concerns
- Poor decision making

To support reliability, data quality controls are incorporated throughout the data lifecycle.

Validation and Verification

Validation processes help identify inconsistencies, duplication and anomalies.

Depending on the dataset and jurisdiction, controls may include:

- Cross-verification
- Identity matching
- Quality checks
- Consistency reviews

These activities support confidence in the information being utilised.

Deduplication

Duplicate records can reduce accuracy and increase operational inefficiencies.

Deduplication processes help improve data quality by identifying and managing duplicate information where appropriate, including referencing historical data to identify persistent identities.

Data Refresh Cycles

Information changes over time. Addresses change. Contact details change. Corporate relationships evolve.

To maintain relevance, data refresh processes are implemented where appropriate.

Refresh activities help improve accuracy and support ongoing reliability, while historical data strengthens identity resolution by capturing and sharing changed data attributes, such as contact details.

Ongoing Monitoring

Data quality is not assessed only at onboarding.

Ongoing monitoring activities help identify:

- Emerging quality issues
- Supplier performance concerns
- Regulatory developments
- Operational risks

Monitoring supports continuous improvement and accountability.

Governance and Oversight

Data sourcing and quality activities are supported through governance and oversight structures.

Oversight may involve:

- Compliance reviews
- Privacy assessments
- Risk management activities
- Supplier governance processes
- Internal assurance reviews

This governance framework helps ensure sourcing decisions remain aligned with organisational standards and customer expectations.

Supporting Regulated Organisations

Many of our customers operate within highly regulated sectors where supplier oversight is a regulatory expectation rather than a commercial preference.

Financial institutions, fintechs, payment providers and public sector organisations must be able to demonstrate that third-party suppliers are subject to appropriate governance and assurance processes.

Our sourcing and quality framework is designed with these requirements in mind.

Frequently Asked Questions

Where does your data come from?

Data may originate from government-linked sources, telecommunications data, authorised partners and other legally permissible sources, depending on jurisdiction and legal availability.

How do you assess suppliers?

Suppliers undergo due diligence covering legal authority, privacy compliance, security controls, governance maturity and data quality processes.

Do you verify data quality?

Yes. Validation, verification, deduplication and monitoring activities help support quality and reliability.

Do you use anonymous or unverifiable sources?

No. Traceability and accountability are fundamental requirements within our sourcing framework.

Why is ethical sourcing important?

Ethical sourcing helps organisations maintain trust, reduce reputational risk and demonstrate responsible data governance.

Conclusion

> *Trustworthy identity intelligence begins with trustworthy data.*

Through structured supplier due diligence, governance oversight, quality controls and ethical sourcing principles, 1datapipe seeks to provide enterprise organisations with confidence that the information supporting their decisions is obtained responsibly and managed appropriately.

As regulatory expectations continue to evolve, organisations must be able to demonstrate not only what data they use, but why they trust it. Our approach is designed to help customers meet that expectation through transparency, accountability and continuous improvement.