Enterprise Trust Centre Guide

Governance, Compliance, Privacy and Accountability at 1datapipe

Table of Contents

Introduction

Organisations operating in regulated environments face increasing scrutiny over the suppliers they engage, the data they utilise and the decisions they make. Regulators, auditors, procurement teams and customers all expect organisations to demonstrate that data is sourced responsibly, processed lawfully and governed effectively.

At 1datapipe, trust is not treated as a marketing concept. It is embedded into our operating model through governance, compliance, regulatory oversight, privacy management and information security controls.

This guide provides an overview of the principles, controls and governance structures that underpin our services and explains how we support enterprise customers in meeting their own regulatory, risk and assurance obligations.

Our Approach

1datapipe provides identity intelligence solutions designed to support fraud prevention, identity verification, customer onboarding, compliance monitoring and risk management activities.

We recognise that access to data alone is not enough. Enterprise customers require confidence that data is sourced responsibly, processed lawfully and managed through appropriate governance controls.

Our approach is built around five core principles:

- Lawfulness
- Transparency
- Accountability
- Security
- Data Quality

These principles influence how we evaluate suppliers, develop products, manage risk and support customers.

Governance by Design

Governance is integrated throughout our business rather than operating as a separate compliance exercise.

Oversight is provided through our Compliance, Regulatory and Data Protection (CRDP) function alongside Information Security, Legal and Operational stakeholders.

This governance framework is designed to ensure:

- Regulatory obligations are identified and assessed.
- Privacy considerations are incorporated into decision making.
- Risks are identified and managed appropriately.
- Policies and procedures remain current.
- Customers receive consistent and defensible responses to due diligence enquiries.

Governance activities include:

- Regulatory horizon scanning

- Risk assessments
- Policy management
- Internal reviews
- Control monitoring
- Customer assurance support

This approach enables 1datapipe to maintain consistency whilst responding to evolving legal, regulatory and customer expectations.

Lawful Processing and Legitimate Interest

One of the most common questions we receive from customers concerns the lawful basis used for processing data.

Where permitted by applicable legislation, 1datapipe relies on legitimate interest as the lawful basis supporting relevant processing activities.

Legitimate interest is recognised under privacy frameworks including the UK GDPR and EU GDPR as a valid lawful basis where processing is necessary, proportionate and balanced against the rights and freedoms of individuals.

For identity infrastructure providers, legitimate interest often provides the most appropriate lawful basis because organisations, government bodies and law enforcement agencies require reliable methods to:

- Prevent fraud
- Verify identities
- Reduce financial crime
- Support onboarding activities
- Improve risk management processes
- Protect customers and organisations from harm
- Investigate criminal activity

Why Consent Is Not Used

Customers frequently ask why consent is not obtained from every individual whose data may be included within identity infrastructure datasets.

While consent is an important lawful basis in certain circumstances, it is not always the most appropriate or practical basis for identity verification, fraud prevention and risk management activities.

Reliance on consent can create significant operational challenges whilst potentially reducing the effectiveness of fraud prevention controls and identity verification processes.

Instead, 1datapipe assesses processing activities against applicable legal requirements and utilises lawful bases that are appropriate for the nature, purpose and context of the processing.

Legitimate Interest Assessments

To support accountability, documented Legitimate Interest Assessments (LIAs) are undertaken where appropriate.

These assessments typically consider:

Purpose Test

Why is the processing taking place?

The assessment examines the business objective and whether that objective is lawful, legitimate and clearly defined.

Necessity Test

Is the processing necessary?

This stage evaluates whether the intended outcome can reasonably be achieved through less intrusive means.

Balancing Test

What is the impact on individuals?

The assessment considers:

- Reasonable expectations
- Potential privacy impact
- Safeguards implemented
- Rights available to individuals
- Overall proportionality

The objective is to ensure that legitimate business interests do not override the rights and freedoms of individuals.

Privacy Governance

Privacy governance forms a key component of our operational framework.

Privacy considerations are integrated into business processes through:

- Data Protection Impact Assessments (DPIAs)
- Privacy reviews
- Policy frameworks
- Supplier due diligence
- Regulatory monitoring
- Data subject rights procedures

Privacy governance is not treated as a one-time exercise. Controls and assessments are reviewed periodically to reflect changes in processing activities, regulatory expectations and customer requirements.

Data Subject Rights

Individuals are afforded various rights under applicable privacy laws.

Depending on jurisdiction and circumstances, these may include:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restriction
- Right to object
- Rights relating to automated decision making

Requests are managed through documented procedures designed to ensure consistency, accountability and compliance with applicable legal requirements.

Data Sourcing and Ethical Data Acquisition

> *Trust in data begins with trust in its source.*

1datapipe maintains a structured approach to supplier onboarding and data sourcing designed to support legal compliance, transparency and quality.

Potential suppliers are evaluated against a range of criteria including:

- Legal authority to provide data
- Compliance maturity
- Privacy controls
- Security controls
- Data quality processes
- Contractual commitments

We seek to ensure that data sources are traceable, supportable and aligned with applicable legal requirements.

Data Quality Controls

Data quality is critical for organisations relying upon identity intelligence.

To support quality and reliability, controls may include:

- Validation processes
- Data verification
- Deduplication
- Data refresh cycles
- Ongoing supplier monitoring
- Quality assurance reviews

While no dataset can always guarantee absolute accuracy, these controls help support confidence in the information provided.

International Data Transfers

Many enterprise organisations operate across multiple jurisdictions and therefore require assurance regarding international transfers.

Where applicable, cross-border transfer mechanisms are implemented in accordance with relevant legal requirements.

Depending on jurisdiction, these may include:

- Standard Contractual Clauses (SCCs)
- Transfer Impact Assessments (TIAs)
- Local contractual provisions
- Country-specific compliance measures

Transfer requirements are monitored as part of our broader privacy governance programme.

Regulatory Monitoring

The regulatory environment continues to evolve rapidly.

New privacy laws, AI regulations, cyber security requirements and operational resilience expectations are emerging across multiple jurisdictions.

To support ongoing compliance, regulatory monitoring activities include:

- Horizon scanning
- Legal updates
- Regulatory guidance reviews
- Impact assessments
- Internal control updates

This enables regulatory developments to be assessed and incorporated into governance processes where appropriate.

Information Security

Privacy and governance are only effective when supported by strong security controls.

Security measures are designed to protect confidentiality, integrity and availability.

Controls may include:

- Encryption in transit and at rest
- Access management controls
- Role-based permissions
- Monitoring and alerting
- Vulnerability management
- Security testing
- Incident response procedures

Security governance is supported through documented policies, standards and oversight activities.

Incident Management

Despite preventative controls, organisations must be prepared to respond effectively to incidents.

1datapipe maintains documented incident response procedures designed to support:

- Detection
- Investigation
- Containment
- Remediation
- Regulatory notification where required
- Continuous improvement

Lessons learned from incidents are incorporated into governance and risk management activities.

Customer Assurance and Due Diligence

Enterprise customers frequently conduct detailed reviews of suppliers before engagement.

To support these reviews, 1datapipe can provide information relating to:

- Governance frameworks
- Privacy controls
- Security controls
- Regulatory compliance programmes
- Risk management activities
- Due diligence processes

The objective is to enable customers to make informed decisions and satisfy their own governance obligations.

Supporting Regulated Organisations

Many of our customers operate in highly regulated sectors including:

- Banking
- Financial services
- Fintech
- Payments
- Telecommunications
- Government and law enforcement
- Public sector organisations

These organisations face increasing expectations regarding third-party risk management, operational resilience, data governance and accountability.

Our governance framework is designed with these expectations in mind.

Conclusion

> *Trust must be earned through evidence, governance and accountability.*

At 1datapipe, governance, compliance, privacy and security are integrated into the way we operate. Through structured oversight, documented controls and continuous improvement, we aim to provide enterprise customers with confidence that our services are supported by a robust and defensible governance framework.

As regulatory expectations continue to evolve, we remain committed to maintaining high standards of compliance, transparency and operational integrity whilst supporting customers in achieving their own governance and assurance objectives.