

COMPLIANCE FAQS

Frequently Asked Questions

Compliance, Privacy, Security and Governance

CONFIDENTIAL · ©2026 IDENTIA · ALL RIGHTS RESERVED

Table of Contents

01	About Identia	2
02	Data Sources and Quality	2
03	Privacy and Lawful Basis	3
04	Security and Operational Resilience	3
05	Governance and Compliance	4
06	International Transfers	4
07	Customer Due Diligence	5
08	Final Assurance	5

© 2026 Identia. All rights reserved.

01

About Identia

What does Identia do?

Identia provides identity intelligence and identity infrastructure solutions that support fraud prevention, identity verification, customer onboarding, risk management, government and law enforcement investigations and compliance activities.

Who are our typical customers?

Banks, lenders, fintechs, payment providers, insurers, telecommunications companies, government agencies and other regulated organisations.

How is Identia different from a traditional data broker?

Identia operates as an identity infrastructure provider, supporting risk, fraud, verification and compliance use cases through governed and auditable identity intelligence.

02

Data Sources and Quality

Where does our data come from?

Data originates from two primary source categories:

Government & Public Authority Records

Official government and public-sector registries accessed through authorised and compliant channels. These records form the foundation of the identity graph and establish high-confidence core identity attributes such as legal identity, registration status and address history.

Telecommunications-Grade Reference Data

High-quality telecommunications-grade reference sources used solely to corroborate, validate and refresh core identity attributes within the graph. These sources are not used for behavioural analysis, monitoring or decisioning.

How do we assess data suppliers?

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

Do we use scraped data?

No. We do not utilise unlawfully obtained, unverifiable or anonymous data sources.

© 2026 Identia. All rights reserved.

How do we ensure data quality?

Data quality is supported through validation, verification, deduplication, refresh cycles and ongoing supplier monitoring.

Do we process sensitive personal data?

No. We do not knowingly process special category or sensitive personal data requiring explicit consent.

03

Privacy and Lawful Basis

What lawful basis do we rely on?

Where permitted by applicable law, Identia relies on legitimate interest as the lawful basis for relevant processing activities.

Why do we not rely on consent?

For identity verification, fraud prevention and risk management activities, consent is not always the most appropriate or effective lawful basis.

Do we complete Legitimate Interest Assessments?

Yes. Assessments are undertaken where appropriate to evaluate purpose, necessity, proportionality and safeguards.

Do individuals have privacy rights?

Yes. We support applicable data subject rights in accordance with relevant privacy legislation.

Do we conduct Data Protection Impact Assessments (DPIAs)?

Where appropriate, DPIAs are undertaken to assess and mitigate privacy risks.

04

Security and Operational Resilience

How do we protect data?

Security controls include encryption, access management, monitoring, vulnerability management, incident response procedures and employee awareness programmes.

Do we have an incident response process?

Yes. We maintain documented procedures for identifying, investigating, containing and remediating incidents.

© 2026 Identia. All rights reserved.

How do we manage operational resilience?

Through governance, business continuity planning, resilience testing and risk management activities.

Do we monitor security risks?

Yes. Security risks are assessed and managed through structured governance and risk management processes.

Are employees trained on security and privacy obligations?

Yes. Awareness and training programmes form part of our governance framework.

05

Governance and Compliance

How do we monitor regulatory change?

Through horizon scanning, regulatory monitoring, impact assessments and governance reviews.

What is the CRDP framework?

Our Compliance, Regulatory and Data Protection framework integrates governance, privacy, compliance and risk management activities into a unified oversight model.

How do we manage compliance risk?

Through risk assessments, policy governance, monitoring activities and management oversight.

Who oversees compliance and privacy?

Dedicated governance functions provide oversight of compliance, regulatory and privacy obligations. The team is headed by our Chief Compliance Officer and Group DPO.

How do we demonstrate accountability?

Through documented controls, governance reporting, assessments, audits and ongoing monitoring.

06

International Transfers

Do we store and transfer data internationally?

We store data in AWS Europe or country of origin if required. Where necessary and legally permissible, international transfers may occur in accordance with applicable legal requirements.

© 2026 Identia. All rights reserved.

How do we safeguard international transfers?

Appropriate transfer mechanisms may include Standard Contractual Clauses (SCCs), Transfer Impact Assessments (TIAs) and other recognised safeguards.

07

Customer Due Diligence

Do we support customer due diligence reviews?

Yes. We regularly support procurement, legal, privacy, compliance and security assessments.

Can supporting documentation be provided?

Subject to confidentiality and contractual requirements, supporting governance, privacy, compliance and security documentation may be made available.

Do we complete customer questionnaires?

Yes. We routinely support enterprise due diligence and onboarding processes.

Can customers speak with our Compliance or Privacy teams?

Yes. Subject matter experts are available to support customer assurance activities where appropriate.

08

Final Assurance

Why do enterprise organisations choose Identia?

Because they require more than data. They require governance, accountability, transparency and confidence that their supplier can withstand regulatory, audit and due diligence scrutiny.

What is our overall approach to trust?

Trust is built through lawful processing, responsible sourcing, strong governance, effective security controls and continuous oversight.

© 2026 Identia. All rights reserved.