THE COMPLIANCE BRIEFING
PRACTICAL INTELLIGENCE FOR COMPLIANCE PROFESSIONALS
INTELLIGENCE NOTE

AML & DATA PRIVACY

Data Privacy and AML: *Not Competing, But Not Simple Either*

The question of whether data privacy law conflicts with anti-money laundering obligations comes up regularly in training rooms and compliance forums. The short answer is no. The more useful answer is that it is complicated, and the complications are worth understanding.

Most compliance professionals already know that anti-money laundering (AML) obligations justify processing personal data. What is less settled in practice is proportionality: how much data is genuinely necessary, how long it should be retained, who can access it, and what happens when an individual asserts rights under data protection law. These are not theoretical edge cases; they arise in real compliance programmes.

01

The Legal Framework in Plain Terms

The Information Commissioner's Office (ICO) has confirmed that AML obligations constitute a lawful basis for processing personal data under UK law. The key provisions are Article 6(1)(c) of the UK General Data Protection Regulation (UK GDPR), covering processing necessary for compliance with a legal obligation, and Schedule 1, Part 2, paragraph 10 of the Data Protection Act 2018, which expressly addresses anti-money laundering.

Identity verification, customer risk assessment, transaction monitoring, and suspicious activity investigation are all lawful data processing activities when conducted under the relevant AML legislation. The Financial Action Task Force (FATF) has published specific guidance confirming that AML obligations can and should be implemented consistently with privacy requirements.

The operative principle is proportionality: collect only what is necessary, retain it only as long as required, protect it appropriately, and restrict access to authorised personnel. These are data protection principles, but they are also good AML governance.

02

Where It Gets Genuinely Hard

Three practical scenarios generate the most friction in live compliance programmes.

A publication of FCC Consulting Ltd. For information purposes only. Does not constitute legal or regulatory advice.

SARs and Subject Access Requests

When a firm files a Suspicious Activity Report (SAR) with the National Crime Agency (NCA), the tipping-off provisions of the Proceeds of Crime Act 2002 prohibit disclosure to the subject. If that individual then submits a subject access request under UK GDPR, firms cannot confirm the SAR's existence, but they cannot simply ignore the request either. A clear documented protocol is essential before this situation arises, not while it is happening.

Retaining CDD Data

The 2017 Money Laundering Regulations require five-year retention of customer due diligence (CDD) records after a business relationship ends. Complications arise when customers request erasure under UK GDPR, or when retention beyond the standard period is needed for an ongoing investigation. A blanket policy of indefinite retention satisfies neither regime.

Cross-Border Transfers

Group-wide AML programmes and correspondent banking require sharing personal data across borders, creating direct tension with UK GDPR transfer restrictions. Adequacy decisions, standard contractual clauses, and binding corporate rules each provide a legal pathway, but firms routinely treat them as a tick-box exercise rather than a substantive governance question.

0 3

Privacy-Enhancing Technologies: Emerging Tool, Not a Fix

Privacy-Enhancing Technologies (PETs) are increasingly relevant as AML moves towards greater orchestration and collaborative risk management. The Bank for International Settlements (BIS) Project Aurora has been exploring how PETs can support cross-border AML monitoring while reducing direct exposure of personal data.

The following techniques can allow institutions to identify risk indicators or detect criminal networks without directly sharing underlying personal data:

Technique	Description	Example Application in AML
Federated Learning	A machine learning approach in which models are trained across multiple institutions' datasets without any raw data leaving each organisation. Each party trains locally; only model updates are shared and aggregated centrally.	Multiple banks jointly train a transaction monitoring model to improve detection of money mule networks, without any bank exposing its customer transaction data to the others.

A publication of FCC Consulting Ltd. For information purposes only. Does not constitute legal or regulatory advice.

Secure Multi-Party Computation	A cryptographic technique that allows two or more parties to jointly compute a function over their combined inputs while keeping each party's input private. No single participant sees the other's underlying data.	Two correspondent banks identify whether a common customer appears on both their internal watchlists, confirming a match or non-match without either disclosing the full list to the other.
Homomorphic Encryption	Encryption that allows computations to be performed directly on encrypted data, producing an encrypted result that, when decrypted, matches the outcome of the same computation on the plaintext. Data remains encrypted throughout processing.	A financial intelligence unit performs risk scoring across encrypted customer records held by a bank, returning only the risk scores, never accessing the underlying personal data in readable form.
Data Pseudonymisation	The replacement of directly identifying information (name, account number, date of birth) with artificial identifiers, so that data can no longer be attributed to a specific individual without reference to separately held mapping information.	A consortium of firms shares pseudonymised transaction patterns with a central analytics platform to detect typologies such as layering. Individual customer identities are not exposed; re-identification is controlled and permissioned.
Trusted Execution Environments	Hardware-level secure enclaves, isolated processing areas within a chip, where code and data can be processed in a protected environment that is verifiably inaccessible to the host system or external parties.	A RegTech platform analyses client data on behalf of a regulated firm within a secure enclave, allowing the firm to verify the integrity of the analysis without the platform operator being able to access or exfiltrate the underlying data.
Differential Privacy	A mathematical framework that adds carefully calibrated statistical noise to datasets or query results, so that the output cannot be used to infer information about any individual record, while preserving the aggregate statistical accuracy of the data.	A supervisor requests aggregate typology data from a sector. Firms respond with differentially private outputs that reveal meaningful sector-wide patterns without allowing the supervisor to infer details about any individual customer or transaction.

The critical caveat is that PETs do not replace legal frameworks or governance. They are technical tools that reduce the privacy cost of AML collaboration; they still require a lawful basis for processing, appropriate oversight, and clear accountability. The future question for AML programmes is not whether data can be shared, but how it can be shared safely.

0 4

Questions MLROs Should Be Asking Their DPOs

These questions provide a practical starting point for structured dialogue between the Money Laundering Reporting Officer (MLRO) and the Data Protection Officer (DPO).

- Do we have a documented protocol for handling subject access requests that may overlap with live SAR filings or ongoing investigations?
- Is our CDD data retention policy clearly linked to our legal obligations under the 2017 Regulations, with documented justification for extended retention?

A publication of FCC Consulting Ltd. For information purposes only. Does not constitute legal or regulatory advice.

- Have we mapped all cross-border personal data flows within our AML programme and confirmed the applicable transfer mechanisms?
- Where we use third-party AML platforms or consortium intelligence services, have we assessed their data processing terms and ensured our legal basis extends?
- Are we proportionate in what we collect, and is there CDD data we hold by habit rather than by requirement?
- Have we assessed whether any PET-based solutions could reduce the privacy cost of our AML data sharing arrangements?

THE BOTTOM LINE

AML compliance and data privacy are not competing objectives. They are both obligations, and both must be met. The firms that manage this well do not treat them as separate compliance workstreams; they build programmes in which AML teams and data protection functions understand each other's requirements and work from a shared governance framework.

The practical test for any AML programme is not whether it has a legal basis for processing personal data, as it almost certainly does. The test is whether it can demonstrate proportionality, sound data governance, and readiness to handle the points where the two regimes genuinely pull in different directions.

Sources and Further Reading

1 ICO, 'Data protection and anti-money laundering' — ico.org.uk
2 UK GDPR Article 6(1)(c) and DPA 2018, Schedule 1, Part 2, para 10 — legislation.gov.uk
3 FATF, 'Guidance on Privacy and AML/CFT Measures' (2020) — fatf-gafi.org
4 BIS, 'Project Aurora: Harnessing the power of PETs' (2023) — bis.org
5 JMLSG Guidance, Part I, Chapter 5 (CDD retention obligations) — jmlsg.org.uk
6 POCA 2002, ss.333A to 333E; ICO right of access exemptions — legislation.gov.uk

Michael Harris
Director, FCC Consulting Ltd | AML and Financial Crime Specialist
michael.harris@fccconsulting.co.uk | thecompliancebriefing.co.uk

A publication of FCC Consulting Ltd. For information purposes only. Does not constitute legal or regulatory advice.