Shift from KYC to KYD: The Rise of the Data Aware Compliance Function

February, 2026

Know Your Customer (KYC), as the term suggests, is understanding who the customer is. It is a fundamental, ethical and regulatory requirement in the financial industry. It involves collection of customer information, performing basic verification of who the customer claims to be and trusting that information as the ultimate source of truth for the rest of the financial life of the customer at the institution. This information is most often declared by the customer at the time of the customer onboarding process. In the past, banks and FIs believed that this process was enough to meet the compliance requirements.

With the rise in technology and emerging formats of financial crime, it has been observed that over time, the data gathered for KYC at the time of customer onboarding loses its relevance and accuracy. Relying on this data alone as the ultimate truth is proving to be a huge compliance risk. As we move into the era of RegTech 3.0, the financial industry is transitioning from focusing solely on customer identity verification to a broader, data-centric approach, shifting from *KYC* to *KYD* (*Know Your Data*). This is achieved not just by relying on the information that the customer shared about themselves, but through other means of data - through their universal digital footprint - social media presence, adverse media publishings, transactions patterns etc. Institutions now aim to build a digital profile of the customer with the vast amount of data generated by customers outside of what they have declared. This evolution marks a significant change in the compliance landscape - Shift from KYC to KYD.

KYD enabling Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)

- Social Media and Online Presence: Platforms like LinkedIn, Facebook, and Twitter reveal history, networks, and lifestyle inconsistencies.
- Screening: Automated tools scan news, sanctions lists, adverse media lists, local lists and red flags PEPs (Politically Exposed Persons).
- Transaction Data and Behavioral Analytics: Patterns in spending, geolocation, and login habits flag deviations from usual behavior.

Why is KYD a Good Idea ?

- Better Decision-Making: Diversity in the data enables more informed choices.
- Improved Regulatory Compliance: It helps organizations adhere to complex and emerging regulations.

- Risk Reduction: What one source of data may not reveal can be uncovered from a different source. Identifying and mitigating risks becomes more specific and more effective.
- Enhanced Customer Profiling: Expanding the breadth and depth of customer data empowers organizations to move beyond generic segmentation toward predictive profiling.

The DPDP Act - A New Complexity Layer in Compliance

The Digital Personal Data Protection (DPDP) Act 2023 (Rules 2025) is a comprehensive data privacy law. The aim of this Act is *to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes, and for matters connected therewith or incidental thereto.* This law sets strict rules on collection, storing, processing and sharing of personal data.

All data collecting and data processing platforms are adapting to India's Digital Personal Data Protection (DPDP) Act, 2023, by shifting from broad, complex terms of service to explicit, user-centric consent models. Consequently, fulfilling the Compliance function obligations under new standards are going to become more challenging.

Rules to comply with -

Explicit, informed consent: Personal information of customers for AML/KYC processing is often a legitimate use (no consent required if mandated by regulators), but the FI must ensure that confidentiality guidelines are adhered to.

Purpose limitation: Data collected for AML/KYC must only be used for that compliance purpose, not for unrelated activities.

Data minimization: Processes must collect only the data necessary to meet AML obligations, avoiding excessive or irrelevant data fields.

Accuracy obligation: Ensure customer data is up-to-date and correct through validation and verification processes, reducing the risk of false alerts or incorrect profiling.

Retention & erasure: AML regulations dictate specific data retention periods (5 years extendable to 10 where required), after which data must be deleted. Systems should track retention timelines and deletion actions.

Cross-border restrictions: Data can be processed overseas but records must be maintained. Transfers to government blacklisted countries must be prevented.

Breach notification: If AML/KYC data is compromised, the institution must notify the Data Protection Board and affected customers without undue delay.

Significant Data Fiduciary (SDF) compliance: Large banks/fintechs may be classified as SDFs, requiring a Data Protection Officer, regular privacy audits, and data protection impact assessments for AML processes.

The shift from Know Your Customer (KYC) to Know Your Data (KYD) raises the responsibilities of an organization's compliance function. This evolution demands a proactive approach, new process and deeper data understanding, positioning the organization as a key figure in fostering a data-enabled compliance culture. The introduction of the Digital Personal Data Protection (DPDP) Act in India significantly adds

to this complexity by mandating stringent requirements for lawful data processing, consent management, and breach notification, forcing organizations to not only *know* their data but also meticulously *govern* it in line with the new legal framework.

Quantum Data Engines is a reg-tech company that helps financial institutions detect, manage, and report financial crime more effectively and efficiently.

For more details write to: connect@qde.ai