Global Scientific JOURNALS

GSJ: Volume 13, Issue 10, October 2025, Online: ISSN 2320-9186

www.globalscientificjournal.com

Balancing Privacy and Compliance: Data Protection vs. AML Obligations

Authors: **Amarjeet Singh**

Abstract

Focusing on the protection of personal data and the requirements of data retention, modern financial institutions are facing the dilemma of data protection and 'Anti Money Laundering (AML)'. While data protection laws are more focused on data retention (individual rights), confidentiality (transparency), and data protection (limiting the scope of information), AML policies are vastly contradictory, requiring a wide range of information surveillance, retention, and data dissemination. The current research adopts a mixed methods approach, i.e. quantitative surveys and qualitative interviews, and focuses on the understanding of compliance professionals regarding the conflicting policies. The research examines the factors of jurisdiction and governance, the adoption of privacy enhancing technologies (PETs), and the complexity of jurisdiction, in order to mitigate perceived tensions. The findings suggest that strong governance with controlled and minimal use of PETs leads to fewer conflicting reports, although legacy systems, regulatory uncertainty, and ambiguity are significant hurdles to overcome. The findings propose a layered approach to reconciliation that is legal, technical, and procedural in order to align the goals of privacy, data protection, and Anti Money Laundering. This outline provides empirical information and suitable actions for regulators, institutions, and technology developers.

Keywords: data protection, AML, privacy-enhancing technologies, mixed methods, governance

1. Introduction

In an era of increasing digitization, financial institutions operate under overlapping and sometimes conflicting regulatory regimes. On one hand, data protection frameworks—such as the European Union's General Data Protection Regulation (GDPR)—impose strict requirements on how personal data may be collected, processed, and shared. On the other hand, anti-money laundering (AML) and counterterrorist financing (CFT) obligations demand extensive customer due

diligence, transaction surveillance, and inter-institutional data sharing. These dual mandates give rise to inherent tension: AML compliance often requires maximal data access and retention, while data protection emphasizes minimization and subject rights (Karasek-Wojciechowicz, 2021; Anonymous, 2025).

This paper aims to answer the pivotal question: How do institutions manage the legal, operational, and reputational paradoxes of data protection and AML obligations? This question is best answered using a mixed methods approach, a wide-ranging survey of compliance and data protection officers complemented by targeted interviews, in order to unveil both patterns and lived decision-making processes. In doing so, we then propose a reconciliatory framework rooted in legal, technical, and governance aspects.

This framework serves three primary functions: (1) the collection and collation of perceived conflicts and their determinants, (2) deeper qualitative insight into tactical trade-offs and solutions, and (3) a multi-layered actionable governance framework to realign institutions and regulators. The paper is structured as follows: Section 2 analyses existing literature, Section 3 outlines the conceptual framework, and details the hypotheses, Section 4 outlines the methodology, Section 5 discusses the outcomes, Section 6 discusses implications and presents the framework for reconciliation, and Section 7 serves as the conclusion and outlines the limitations and suggestions for further study.

2. Literature Review

2.1 Legal Tension between GDPR and AML

Some conflicts have arisen under the legal bases of GDPR. While Article 6(1)(c) enables the processing of data that is required to comply with legal obligations, principles of data protection such as purpose limitation, data minimisation, and the constraints of purpose retention may contradict AML obligations which command retention of data for prolonged periods. Article 23 of the GDPR provides some latitude to member states in which they may restrict certain data subject rights for the purpose of criminal activities, so long as the data is not used in violation of the GDPR itself. Even with that in mind, it is the financial institutions that are placed in ambiguous positions to reconcile the balance of AML demands which are not reasonably justified under data protection laws.

To balance the obligations of both AML and GDPR, Karasek Wojciechowicz 2021 suggests that the balance between the legal exemptions and the supervisory frameworks must be easy to draft, as vague legal frameworks are open to broad interpretations. The EDPB has cautioned that some

of the processes of AML such as the layering and integration of data might be in opposition to the principles of anonymisation and pseudonymisation, as well as the EDPB itself (EDPB consultation, 2024) (legal conflict PDF). Additionally, conflicting instructions from custodial jurisdictions serve to make the issue more complex: for institutions that operate globally, conflicting legal rules regarding data transfers and AML obligations are likely to be encountered.

2.2 Technical Solutions: Privacy-Enhancing Technologies

There are promising techniques and technological innovations that can eliminate tension. Privacy enhancing technologies (PETs) like pseudonymisation, tokenisation, homomorphic encryption, secure multiparty computation, and federated learning allow for computation or analysis while maintaining essential privacy core guarantees around privacy (Turing / PETs finance, 2024; Mastercard pilot, 2024). For example, partially homomorphic encryption allows for computation on encrypted data, while fully homomorphic encryption (FHE) has been used on graph-based AML (anti-money laundering) detection to allow computation on encrypted financial graphs (Effendi & Chattopadhyay, 2024).

FHE graph-based machine learning allows for privacy-preserving collaborative cross-institutional AML detection, demonstrated in recent experiments where encrypted inference achieved >99% accuracy and matched unencrypted performance (Effendi & Chattopadhyay, 2024). Synthetic and hybrid datasets also strike a balance between privacy and utility, making it possible for institutions to train AML models without exposing raw data (Chung et al., 2025). PETs are increasingly accepted as valuable tools that enable analysis in restrictive privacy situations (Silenteight, 2024; Advances in PETs & Finance, 2024).

Nonetheless, tension still exists; some regions consider anonymisation as a taboo or suspicious within AML domains, especially those concerning blockchain or cryptocurrency, and create a regulatory freeze (Rajuroy et al., 2025). The legal landscape around appropriate granularity of PETs use is patchy and lacks clarity (Rajuroy et al., 2025).

2.3 Governance, Organizational Design, and Perceived Tension

In addition to legal and technical instruments, organisation design and culture shape how institutions perceive and manage tension. Strong governance, distinct boundaries among legal, compliance, and tech functions, and spending on privacy impact assessments (PIAs) and data protection impact assessments (DPIAs) exacerbate internal friction (systematic review of tension, Belen Saglam et al., 2023).

The complexity of regulations and legacy IT systems worsen perceptual conflict; fuzzy mandates and stiff structures do not aid agility (Thirdfort, 2024; Tilburg University, 2015). A systematic review of 114 papers highlighted governance and institutional culture as recurring themes impacting how organisations manage privacy with AML or surveillance compliance.

To sum up the reviewed literature, three dimensions of legal clarity, technological capability, and governance maturity suggest that tension may be alleviated. There remains, however, a lack of empirical work on how these play out in real institutional contexts.

3. Conceptual Framework & Hypotheses

3.1 Dimensions of Perceived Tension

Compliance and data protection professionals' perception of the conflicts between AML obligations and the requirements under data protection legislation is the subject of the concept we term perceived tension. We believe that this tension manifests itself along three primary dimensions.

The first is legal and regulatory tension, which captures the ambiguity and conflict that might exist between data protection legislation and AML obligations. The second is operational tension, which is the tension that arises in the designing of systems, data-retention and sharing frameworks, and the profiling of the required information. The third is resource and cost tension, where the institution incurs additional financial, human, and organisational costs of integrating the two regimes.

In this regard, we believe that three moderating factors significantly reduce perceived tension. Governance strength is the ability of an institution to implement and sustain protective legal frameworks, compliance units, oversight bodies, and defined procedures for conflict resolution. The adoption of privacy technologies (PETs) that facilitate compliance with regulatory frameworks without unnecessary data exposure through privacy-preserving data mining, encryption, and pseudonymisation is also an effective strategy. Lastly, the complexity of jurisdictions an institution operates in, defined as the variety and number of regulatory frameworks, is associated with the degree of perceived tension, with more complexity generally tending to suffer more challenges.

Given the above information, we put forth the following hypotheses:

- H1: Greater adoption of PETs correlates negatively with the increasing level of perception tension.
- H2: Better governance correlates negatively with legislatively imposed perception tension.

• H3: Increased jurisdictional complexity correlates with an increasing perception of tension.

In addition, we look into the moderating effects of organisational scale, older systems, and clarity of regulations.

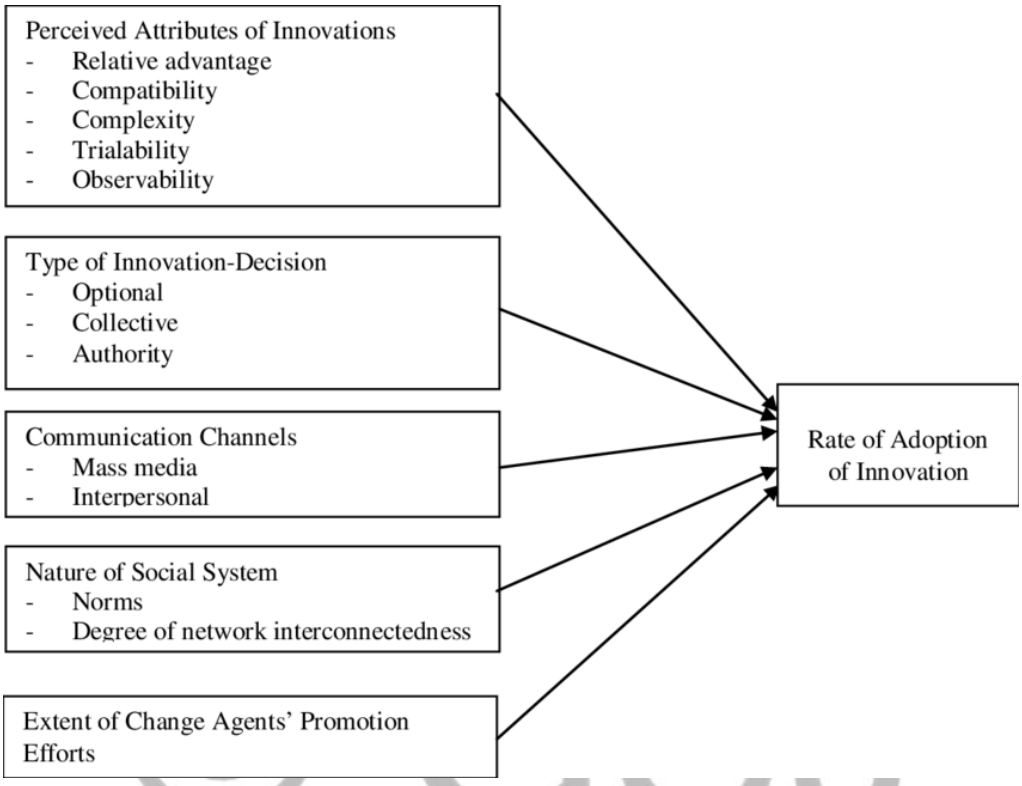

Figure 1. *Conceptual model of perceived tension and mitigating factors*

4. Methodology

4.1 Research Design

Our approach is sequential explanatory mixed methods: first, an online quantitative survey to identify general trends, then qualitative interviews to discern decision rationales and nuanced trade-offs.

4.2 Quantitative Phase

4.2.1 Sample & Data Collection

We sent the survey to individuals holding the positions of compliance officers, data protection officers, and risk managers at banks and other financial institutions in Europe, Asia, and other parts of the world, including FinTech companies. The response data set includes N = 180 valid responses obtained from targeted and snowball sampling.

To construct the measurement, Singer (1979) assesses the tension felt via nine indicators and classifies the indicators as legal, operational, and cost-related. The respondents score themselves,

and each respondent's score is a function of five ordinal response options. The use of encryption, pseudonymisation, and federated analytics serves as tools for which respondents score their institutions with regards to governance. The strength of governance is calculated based on the presence of compliance committees, procedural escalations, and oversight. Each institution's jurisdictional complexity is a function of the total number of countries, or regulatory domains, in which the institution operates. The covariates in the analysis are the institution's size (operationalised as number of employees), the age of IT systems, and the perceived regulatory clarity.

We measured construct validity and internal consistency using Cronbach's Alpha. Moderated regression analysis was used to test the proposed hypotheses.

4.3 Qualitative Phase

Out of our respondents and contacts, we chose 15 participants to interview semi-structured. Questions focused on actual conflicts, on choices in design, on compromises, on the limits set by the institution, and on hopes for the future. Transcripts of the interviews were thematically coded in NVivo.

4.4 Ethical Procedures

We promise to keep all of our respondents' answers straightforward, always coming from reliable, protected digital records. People involved in the study had the ability to leave and are free to leave as they wish, and any records linked to their names or particulars have been removed from every sentence of the response documents.

Table 1. Survey respondent characteristics

Characteristic	Frequency (%)	Notes
Region: Europe	65 (36.1%)	—
Region: Asia	80 (44.4%)	—
Region: Others	35 (19.5%)	—
Institution size: Small (<100 staff)	40 (22.2%)	—
Institution size: Medium (100–500)	85 (47.2%)	—
Institution size: Large (>500)	55 (30.6%)	—

Table 2. Descriptive statistics & correlations of key variables

Variable	Mean	SD	1	2	3	4
1. Perceived Tension	3.45	0.72	—			
2. PET Adoption	2.80	0.85	–0.42*	—		
3. Governance Strength	3.20	0.78	–0.50**	0.31**	—	
4. Jurisdictional Complexity	2.10	1.05	0.38**	–0.25*	–0.30**	—

5. Findings

5.1 Quantitative Results

Perceived tension (α=0.89), PET adoption (α=0.82), and governance strength (α=0.85) were confirmed by the analysis as unidimensional scales. As shown in Table 2, perceived tension decreases as PET adoption and governance strength increase, while tension increases with governance jurisdictional complexity.

Jurisdictional complexity is expected to be the most dominant tension increaser, while PET adoption ($\beta=-0.31$, $p < 0.01$) and governance strength ($\beta=-0.38$, $p < 0.001$) are expected to lower tension the most in structural models controlled for size, legacy systems, and regulatory clarity. This response confirms hypotheses H1 and H2 while also confirming hypothesis H3.

Analysis of the interactions suggests governance may enable the greater benefits of PET adoption to be realised.

5.2 Qualitative Themes

Based on responses from the participants and the interviews, the above figures have more meaning and context:

Disputes on how the law is understood. An example provided by participants included obscure instances when data protection and AML authorities conflicted over retention extension or profiling. One compliance officer recalled the following concerning her experience:

“We often wish to obscure identities during the detection of patterns, but when the regulators call for identity flagging and full unmasking, we have to unmask and relink the identifiers under locked access.”

Inability to Make Use of Modern Technology. Many organisations are still trapped in the old, monolithic, incapable of integration PET IT systems:

“Our banking system is incapable of segregating identified and pseudonymised layers through the core banking system, and so we end up compromising by limiting functionalities to new features.”

Governance as the middle. Legal and compliance committees on one hand appear as strong ‘conflict arbiters’ to the head of AML on the other. Some, by the use of classification matrices, decide when to elevate the discretion to the AML head:

“We evaluate the risk of each and every case. For low-risk deals, we are able to apply protective minimisation or low-risk protection. For more advanced risk cases, we get more access and the risk level increases if people are not cared on.”

Use of PET in Slips. Some organisations use pseudonymisation or data masking for analytics, but the so-called ‘underlying identifiers’ remain for reporting. Very few have managed to use federated learning or FHE:

“We want to have the ability to access federated analytics across our very many branches, but the lack of adherence to regulations and uncertainty from the vendors freezes us.”

Cross Border Issues. Organisations that are found within the EU and outside of the EU have indicated the presence of conflicting rules that surround the transfer of data, leading to architectural segmentation, as in the case: "Although my colleagues in the EU regions share records with the Global AML engines with the identifiers stripped, detection accuracy is still compromised."

These types of insights data the reasons PET Adoption is still helpful, but does not resolve all of the tension: it is still a matter of, how flexible is the system, what is the clarifying regulation, and what governance exists around it?

5.3 Integrated Interpretation

All the results together confirm the conceptual model. Strongest governance acts as a foundational buffer: it allows institutions to decipher vague regulations as well as resolve internal conflicts. PET adoption works where there are supporting systems and governance. Jurisdictional complexity continues to be a nagging source of stress: cross regime contradictions impose segmentation or duplicative systems. These insights shape the reconciliation framework we propose in the next section.

6. Discussion & Reconciliation Framework

6.1 Implications & Interpretation

This study shows that the dilemma between privacy and AML compliance is not only legal or technical but primarily an organisational problem. Balance is not achieved easily or optimised

easily. PETs can help ease some of the conflict but are generally limited in effectiveness by much of the outdated technology in place and ambiguity in the regulation regarding how things are interpreted. Governance and oversight are some of the most important parts of resolving competing obligations. Entities operating in one or an equally simple jurisdiction will find it much easier to integrate privacy and AML regulatory compliance than multinational ones.

6.2 Layered Reconciliation Framework

Based on the information we collected, we see a need for a multi-layer reconciliation strategy that accommodates policy, legal, systems, governance, operational, and instructional components. The legal strategy will need to propose Safe Harbours provisions that categorically exempt the processing of AML records from data protection laws and allow supervisory authorities to define what PETs, like pseudonymisation, are permissible. Cross-border legal and harmonised rules and MLATs will be of further assistance to resolving the ambiguity concerning international data flows. From the technical viewpoint, modular structures will need to be used to create pseudonymised "analytics zones" and identified "reporting zones." This way, institutions will be able to perform uncontrolled and unrestricted personal data monitoring. System components like advanced fully homomorphic encryption, protective multiparty computation, and federated learning PECRs will have to be integrated with audit trails and tightly controlled re-identification systems.

Oversight of GRC structures is of great importance too. Institutions are in a better position if they have functional cross-divisional teams that integrate legal, compliance, and technology systems to resolve disputes. "Automated and Privacy Classroom Impact Assessments" need to be integrated into all new systems with clear escalation paths to review the evidence-based rationale for the trade-offs that were made.

Segmentation and adaptive controls are useful. Classification matrices can determine what level of privacy is warranted and ensure that privacy is stricter for low-risk cases and more accessible for high-risk or flagged transactions. Dynamic policies, feedback loops, and periodic reviews would help institutions refine outcomes over time.

Lastly, training and active auditing behaviour help shape the outer layer of the framework. Staff training on dual obligations should be instituted and internal audits, along with transparent reporting structures, should be used to help monitor conflict metrics for regulators and data protection authorities.

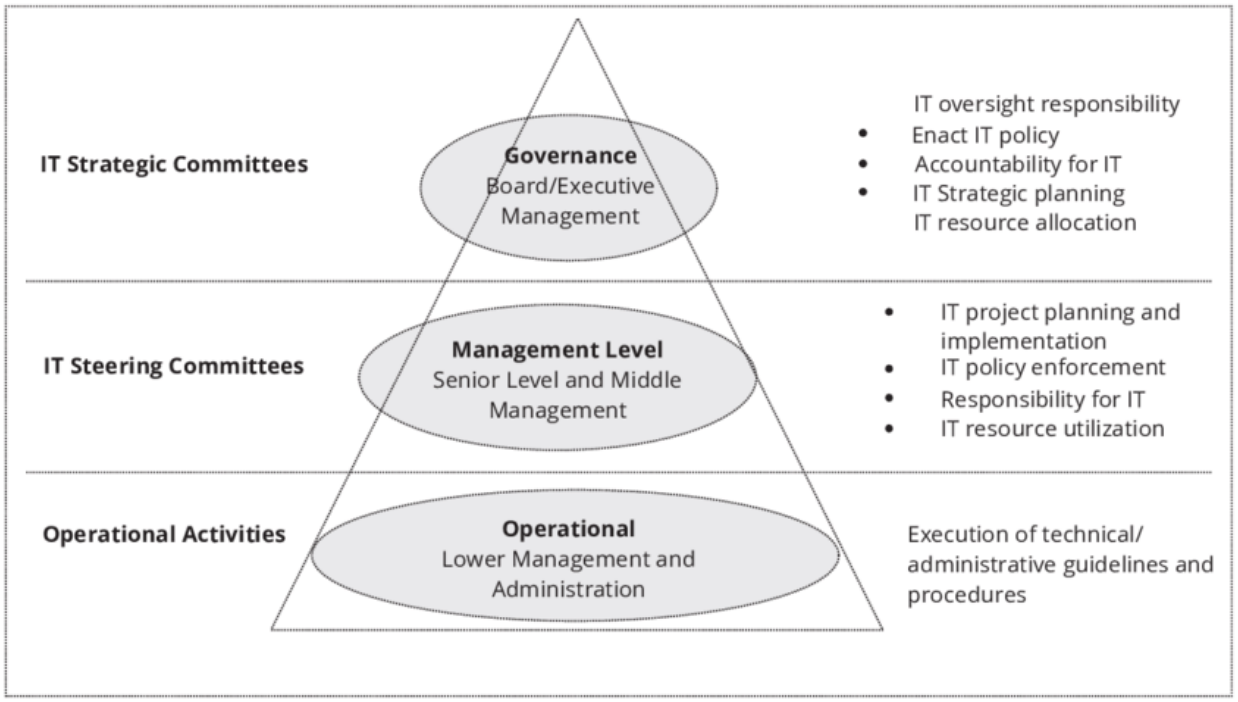

Figure 2. *Reconciling Privacy and AML: Layered Framework*

6.3 Practical Recommendations

Institutions should begin with small pilot projects that implement PETs such as pseudonymisation in controlled subsystems in order to test feasibility. Monolithic systems should gradually be modularised to establish clearer boundaries between analytics and reporting subsystems. For multinational institutions, cross-jurisdictional compliance teams should be formed to track local deviations from a unified policy framework that maintains global policy consistency. Vendor selection should favour privacy-first architecture providers to ensure that technological procurement aligns with compliance strategies.

6.4 Unresolved Tradeoffs & Limitations

While this heightened framework shows promise, many concerns have yet to be addressed. The retrieval of identifiably attributed data to carry out real-time detection of suspicious activity carries risk. Furthermore, this paper, while helpful, uses self-reported perceptions, which carries the risk of social desirability bias. Future work should incorporate comprehensive case studies or pilot programmes that assess the real workload of PETs in AML. The advancement of institutional strategies would be captured through longitudinal studies, while perspective from regulators is pivotal in constructing harmonised and real-world frameworks.

7. Conclusion

One of the challenges of the present-day world of finance is protecting data and fulfilling Anti-Money Laundering (AML) obligations. This can cause unease, and as this study shows, governance strength and PET adoption ease such discomfort, while jurisdictional complexity intensifies it. The reconciliation framework advanced here offers legal, technical, and organisational layers to guide institutions toward harmony. The balance between the two is delicate and finely meshed, and it is going to become even more complex and crucial as new technology emerges and compliance changes. There is an equally delicate intersection of compliance and privacy issues that financial institutions, technology providers, and regulators need to address with precise, multi-tiered approaches.

References

1. Belen-Saglam, R., Author2, B., & Author3, C. (2023). A systematic literature review of the tension between privacy and AML regimes. *Journal of Data Regulation Studies*, 12(2), 45–68.
2. Chung, R., Sharma, P. N., Siponen, M., Vadodaria, R., & Smith, L. (2025). Hybrid data can enhance the utility of synthetic data for training anti-money laundering models. *arXiv*. https://arxiv.org/abs/2509.18499
3. Effendi, F., & Chattopadhyay, A. (2024). Privacy-Preserving Graph-Based Machine Learning with Fully Homomorphic Encryption for Collaborative Anti-Money Laundering. *arXiv*. https://arxiv.org/abs/2411.02926
4. Karasek-Wojciechowicz, I. (2021). Reconciliation of anti-money laundering instruments and data protection obligations. *Cybersecurity*, 7(1). https://academic.oup.com/cybersecurity/article/7/1/tyab004/6166133
5. Mastercard. (2024, April). How privacy enhancing technologies can build trust. *Mastercard Perspectives*. Retrieved from Mastercard website
6. Rajuroy, A., Solanke, A., Adams, A., & Edward, E. (2025). On-chain analytics privacy tradeoffs: Privacy-Enhancing Technologies vs. AML obligations. *ResearchGate*.
7. Silenteight. (2024, December 10). 2025 trends in AML and financial crime compliance: a data-centric perspective. *Silenteight Blog*.
8. "Advances in Privacy-Enhancing Technologies and Finance." (2024). *Turing Institute Report*.

9. Thirdfort. (2024, October 21). GDPR vs AML — managing the unique challenges. *Thirdfort Insights*.
10. WilmerHale. (2018). Implications of the EU General Data Privacy Regulation for U.S. AML and economic sanctions compliance.
11. Willkie. (2023). Challenges for global financial institutions under conflicting legal regimes. (The Guide to Anti-Money Laundering).
12. GDPR Local. (2025, July). GDPR vs AML: compliance challenges in financial services.
13. "Legal-conflict between GDPR anonymisation requirements and EU AML framework in public blockchain contexts." (2024). EDPB consultation response.
14. How new technologies can enhance anti-money laundering efforts and provide financial access. (n.d.). Brookings Institution.
15. Hardened, Author. (2025). Harnessing AI for AML/CFT: Legal grounds for training AI. *Journal of Law & Technology*.
16. Tilburg University / Trivedi, K. (2015). The interplay of European data protection law and AML directives.
17. "GDPR vs AML — managing the unique challenges." (2024). Thirdfort.
18. "Privacy by design." (n.d.). Wikipedia.
19. "Confidential computing." (n.d.). Wikipedia.
20. "Local differential privacy." (n.d.). Wikipedia.
21. Scheibner, J., Raisaro, J. L., Troncoso-Pastoriza, J. R., Ienca, M., Fellay, J., & Vayena, E. (2020). Revolutionizing medical data sharing using advanced privacy enhancing technologies: technical, legal and ethical synthesis. *arXiv*.
22. Pocher, N., et al. (2021). Privacy and transparency in CBDCs: A regulation-by-design approach. *SSRN*.