Dear ladies and gentlemen,

It is possible to build a system where 1) Citizens can use Bitcoin legally and safely, 2) Regulators can trace illicit flows when necessary and 3) GDPR principles like data minimization, user control, and purpose limitation are respected. The tools exist: risk-based KYC, privacy-preserving cryptography, self-sovereign identity, strict data practices. The challenge is political and legal will, and ensuring interoperability between innovation and compliance. Please consider that Bitcoin represents a technological evolution for the secure storage of value. It is regarded as the hardest, most durable and effective form of capital. Such apex capital has always been the foundation of any financial system and the economy. It is a globally needed capability that no entity can stop. Therefore, the EU, its member states, organizations and citizens should be helped to take advantage of its capabilities safely and legally. If we don‘t, we risk falling behind in global financial development, potentially one day ending in debt-serfdom.
The question is: Is a public key personal data? Since MiCA, KYC ensures that wallets, exchanges, and service providers can be monitored when necessary. To enforce rules, authorities need to connect wallet addresses to real individuals. I suggest, that public keys are therefore not personal data, because only the authorities can make that connection. If they are, we should build a system, where the public keys are not personal data.

Regulators must balance:

1. AML/CFT compliance (public interest: prevent crime)
2. DSGVO/GDPR compliance (fundamental rights: privacy, data minimization)
3. Freedom to use Bitcoin legally and safely (technological neutrality & innovation)

These goals can sometimes conflict — e.g., KYC requires identifying people, while GDPR demands privacy and data minimization. So, how could regulators design a system that respects both sides?

Part 1: A Privacy-Preserving, Regulatory-Compliant Framework

1. Tiered KYC / Risk-Based Approach

- Allow low-value or low-risk transactions (e.g. under €100 or €250) with limited or no KYC.
- Require full KYC only for high-risk, high-volume transactions.
- This is already allowed under the EU AMLD5 and MiCA in specific cases.

Benefit: Maintains privacy for small users while enforcing AML for high-risk cases.

2. Zero-Knowledge Proofs (ZKPs) and Privacy-Enhancing Technologies

- Use ZKPs or anonymous credentials to prove legitimacy without revealing identity.
- Example: “Prove I am not on a sanctions list” or “Prove I’m over 18” without revealing full identity.

Satisfies AML checks
Minimizes GDPR exposure
Cryptographic privacy > bureaucratic privacy

3. Decentralized Identity (DID) and Verifiable Credentials

- Use blockchain-based identity systems where users control their data and disclose it selecti vely.
- Service providers can verify credentials without storing raw identity data.

GDPR-friendly (user-centric)
KYC-compliant (verifiable on demand)

4. Strict Data Handling by CASPs

If regulators must enforce KYC:

- Require minimal data collection.
- Enforce data encryption, pseudonymization, and access controls.
- Mandate GDPR-compliant data retention policies (e.g., time-limited).

Respects data protection
Still supports AML compliance

Part 2: Example architecture or policy model

1. Regulated On/Off-Ramps (e.g., Exchanges, Payment Providers)

- Must implement KYC/AML procedures per MiCA and AML laws.
- Must store minimal user data, encrypted and segregated.
- Must offer zero-knowledge KYC verifications (see below).

AML controls happen at entry/exit, not in-network.

2. Decentralized Identity (DID) & Verifiable Credentials

Use standards from W3C DID and Verifiable Credentials with wallets:

- Users complete KYC once with a certified authority (bank, eIDAS, etc.).
- They receive a cryptographic credential proving they're KYC'd.
- Users store this credential in their wallet.
- When accessing a service, they prove:
- "I'm KYC-verified" without disclosing actual identity unless required.

Zero knowledge
GDPR-compliant (data minimization, portability)

3. Transaction Risk Scoring & Tiered KYC

For payments under certain thresholds (e.g., €250), allow:

- Basic wallet usage with pseudonymity
- No KYC beyond network monitoring
- For higher-value or flagged transactions:
- Trigger enhanced due diligence (EDD)
- Require credential-based identity proofs

Balances privacy and AML goals

4. On-Chain Risk Analysis (Optional for Forensics)

Regulators or auditors use blockchain analytics tools to:

- Trace transaction flows
- Identify patterns of laundering
- Link addresses over time

BUT: Use only when probable cause or legal process exists.
No bulk surveillance
Proportional enforcement

I hope this is helpful in the evaluation of an appropriate legal solution for the situation.
Wishing you all the best,
Sincerely, Lorenz Hinteregger