# DARTE SERIES

## Berlin 5.0

Initiated by Mariana de la Roche W. (BlackVogel) and Dr. Nina-Luisa Siedler (siedler legal), the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of MiCAR and expanded to include jurisdiction-specific discussions on data protection, identity, market integrity, and regulatory innovation.

The Berlin 5.0 DARTE edition took place on November 11th, 2025 in collaboration with the European Commission, Project Catalyst, and the Cardano Foundation. This roundtable brought together regulators, legal experts, and blockchain practitioners to explore the intersection of digital identity, privacy, and compliance across both public and permissioned blockchain environments.

The agenda centered on three key themes: the risks and trade-offs in implementing eID frameworks; the challenges of aligning decentralized identity systems with GDPR; and the role of digital ID in KYC/AML regulation. The session opened with welcome remarks from Frederik Gregaard (Cardano Foundation) and concluded with reflections from Dr. Joachim Schwerin (European Commission).

We extend our sincere thanks to all speakers, participants, and institutional partners for their valuable contributions. The views presented in this report reflect the collective understanding of the participants and do not necessarily represent the official positions of individual attendees or rapporteurs.

**Opening remarks by Frederik Gregaard**

The session opened with a keynote by Frederik Gregaard, CEO of the Cardano Foundation, who emphasized the foundational role of digital identity in enabling a secure and inclusive digital economy. He framed identity not merely as a compliance requirement but as a building block for scalable trust and human agency across decentralized systems. Drawing from Cardano's experience supporting identity frameworks in diverse jurisdictions, he underscored the need for regulatory clarity, interoperability between identity providers, and the role of public blockchains in anchoring verifiable credentials without compromising privacy. His remarks set the tone for a day of rich debate on how identity systems can serve both innovation and rights preservation in a fast-evolving regulatory landscape.

The opening reflections noted the persistent tension between user-centric design and data privacy, especially as agentic AI and blockchain-based interfaces become more seamless. Participants emphasized the importance of building trust through auditability, proportionate compliance measures, and greater transparency in digital ID architecture. The group also acknowledged that legal innovation must account for changing user behaviors, especially in contexts where users prioritize experience over control or anonymity.

1. **Risks of eID**

The first topic of the Berlin 5.0 DARTE roundtable presented by Florian Daniel (Westernacher) addressed the systemic and societal risks posed by centralized digital identity systems, particularly in light of recent amendments to the eIDAS regulation. The discussion opened with the warning that centralised architectures, especially when combined with programmable digital currencies like the Digital Euro, may endanger core European values such as privacy, freedom of expression, and self-determination.

Participants acknowledged the convenience and potential efficiency gains of a unified EUDI wallet containing credentials such as ID cards, driving licenses, and academic certificates. However, they stressed that without viable alternatives or opt-out mechanisms, such systems risk becoming coercive by design. Comparative examples were cited: India, where Aadhaar is required for access to government services; the UK, which has introduced eID-based entry controls; and Australia and Greece, where eID is tied to social media access. In each case, participants questioned how privacy rights and the presumption of innocence could be preserved, specifically, how to prevent identity systems from enabling disproportionate surveillance, restricting access to essential services, or creating centralized points of failure that could be exploited by malicious actors or misused by authorities. Proposed safeguards included the implementation of selective disclosure mechanisms (such as zero-knowledge proofs), the adoption of fragmented identity models that prevent the consolidation of user data across contexts, and the creation of decentralized credential issuance networks that distribute trust rather than concentrating it in a single authority. Moreover, participants emphasized the need for revocable and unlinkable identifiers, the ability for users to manage consent at a granular level, and a strong commitment to purpose limitation and data minimization principles.

Legal frameworks, including eIDAS, were seen as flexible enough to accommodate these safeguards, but only if regulators and industry actors commit to implementing privacy-preserving architectures by design, not as afterthoughts.

The conversation further explored how eIDs, while often introduced under the pretext of AML, CTF, or child protection, may become tools of surveillance if embedded in centralized infrastructure. Concerns were raised over government visibility into individuals' digital footprints, especially when cash-based alternatives are phased out.

Participants identified several key technical and governance risks:

- Hacking vulnerability of centralized databases, with the German *elektronische Patientenakte* cited as a precedent for the risks associated with large, sensitive data repositories.
- Transaction traceability across all credential uses, which could enable behavioral profiling, blacklisting, or politically motivated control if misused.
- Accountability gaps in decentralized systems, particularly questions around liability in cases of failure, fraud, or dispute resolution, such as who can revoke access or respond to malicious use.
- Revocation and identity theft emerged as particularly difficult to address in decentralized architectures, where no single authority exists to intervene.

Despite these challenges, the group explored several promising alternatives aimed at preserving privacy and self-determination:

- Leveraging ZKPs to validate individual attributes, such as age, residency, or professional qualification, without revealing full identity or enabling transaction-level surveillance.

- Fragmented, context-specific eIDs where only minimal, relevant credentials are shared depending on the situation. For example, in international law enforcement settings, participants discussed how existing systems like Interpol can request identity-related data across jurisdictions, often with limited transparency or user protections. A privacy-preserving alternative would be to only verify that a person meets a specific criterion (e.g., not flagged in a criminal database or having a valid visa), without disclosing their full identity or unrelated credentials, thus avoiding overreach while still enabling cooperation.

- Designing trust layers for decentralized structures, potentially aligned with the Qualified Trust Service Provider (QTSP) model under eIDAS, where verified nodes provide credentials and can issue or revoke them based on a clear governance framework.

- Using established standardization channels such as ISO and DIN, particularly via the NIA (Standards Committee for Information Technology and Applications), to propose and implement technical standards that safeguard core rights like data minimization, unlinkability, and user control.

Participants proposed building an industry-led identity stack anchored in existing regulatory frameworks but optimized for privacy and user control. Several emphasized the need for a risk-based taxonomy of identity use cases, distinguishing between identity, credentials, and characteristics, and enabling context-specific governance. Disposable eIDs, unlinkable credentials, and revocable permissions were all flagged as areas for further exploration.

Ultimately, the discussion highlighted the importance of distinguishing between control and service. As agentic AI and blockchain-based rails become more widespread, users may not even be aware of the backend infrastructure. Regulators must ensure that the convenience of digital identity does not override citizens' rights

| **Call to actions regarding eID and Digital Identity Risks** |
| --- |
| The key call to actions from the discussion are:<br><br>• **Propose a risk-matrix and taxonomy for eID systems:** Create a classification framework for identity types and usage contexts to inform proportional governance and technology design.<br><br>• **Develop ISO-standard proposals for privacy-preserving digital identity:** Industry stakeholders should coordinate through DIN/ISO to shape globally applicable, decentralized ID standards aligned with fundamental rights.<br><br>• **Encourage fragmented, revocable identity structures:** Promote architectures that allow multiple disposable IDs, context-specific credentials, and revocation mechanisms to reduce surveillance and misuse. |

## 2. Digital IDs on public blockchain & GDPR

The second topic of the session, presented by Nicolas Jacquemart (Cardano Foundation) focused on reconciling digital identity systems on public blockchains with the European Union's data protection framework, particularly the GDPR. The discussion started by addressing the inherent tension between immutable, transparent infrastructures like public blockchains and legal requirements such as the right to erasure, data minimization, and purpose limitation.

Public blockchains are generally not recommended for storing personally identifiable information (PII) due to their append-only nature and universal accessibility. Any data recorded on-chain is potentially permanent and visible to anyone. This raises concerns under GDPR, which mandates that individuals retain rights over their personal data, including the right to rectification and deletion. Yet, the need for identity solutions that ensure accountability and trust in decentralized ecosystems has led to new models attempting to square this circle.

One such model is the Key Event Receipt Infrastructure (KERI), a standard that creates decentralized, self-certifying identifiers and cryptographic event logs (KELs). Instead of storing identity data on-chain, KERI logs key events and changes to identifiers. These logs are verifiable without exposing personal data. The argument presented was that, when properly implemented, the KELs and associated identifiers (AIDs) can be considered anonymous from the perspective of most nodes or observers, provided they lack the legal or technical means to link them to a natural person. In such cases, the GDPR would not apply to the processing of that data by those entities.

Participants debated whether such a system meets the relative or absolute threshold of identifiability under GDPR. Under the absolute approach (favored by some EU regulators), any possibility that someone could identify the data subject means the data is personal, regardless of who processes it. Under the relative approach, the key question becomes whether the specific processor (e.g. a node operator) has the means or legal authority to identify the subject. The relative view was generally preferred by participants, as it enables public blockchain participation without turning every node into a GDPR controller.

In addition, several participants referenced recent CJEU rulings (notably EDPS v SRB) which confirm that identifiability under data-protection law must be assessed in a contextual, actor-specific manner: even pseudonymised or hashed data may remain "personal" if the processor can re-identify, whereas for another actor lacking the means the same data may fall outside GDPR. The Court emphasised the controller's obligation at collection and the 'reasonably likely means' test of re-identification

Beyond identifiability, the session touched on the complexities of how GDPR compliance overlaps with other legal requirements, especially those related to AML and the travel rule. Participants noted that while selective disclosure tools like ZKP and designated-access protocols could help limit unnecessary data exposure, AML frameworks often require full identity verification. This creates a tension: public blockchain architectures are built for transparency and decentralization, while AML enforcement increasingly demands traceability, risk flagging, and data retention.

The debate extended to the governance of these systems. Could a public, permissionless blockchain ever qualify as a "qualified electronic ledger" under eIDAS? While such ledgers would carry compliance obligations similar to qualified trust service providers, the certification process and practical feasibility of qualifying a decentralized infrastructure remains uncertain. Nonetheless, there was optimism that the legal framework allows for layering, building compliant identity services on top of public infrastructure without compromising core decentralization.

Participants also acknowledged practical risks. Even hashed identifiers or metadata patterns on-chain could, with enough auxiliary information, be used to profile users. Examples were raised of blockchain forensics firms mapping wallet behavior and linking accounts through off-chain data, undermining the assumption of pseudonymity. Moreover, use cases involving recovery from lost wallets, family-access credential sharding, and identity revocation were discussed as critical areas where technical innovation must align with user rights and legal safeguards.

Several proposed safeguards and governance mechanisms emerged:

- Create risk matrices and use-case taxonomies to define identity assurance levels, separating low-risk disclosures (e.g., age verification) from high-risk, sensitive attributes (e.g., health or criminal data).
- Encourage disposable and fragmented identity systems that give users control over what is revealed and to whom, minimizing centralized storage or reuse of full identities.
- Promote private-sector-driven standards for digital ID that complement official eIDAS frameworks, giving users interoperable but privacy-preserving tools.
- Recognize the importance of standardization bodies such as ISO and DIN in defining common criteria for selective disclosure, consent revocation, and data minimization.

The discussion closed with calls to harmonize AML and GDPR compliance approaches, noting that the current siloed development of these regimes leads to operational inefficiencies and excessive data exposure. Rather than forcing trade-offs between compliance and privacy, participants advocated for a rights-based design of digital identity systems where selective disclosure and auditability are not just technically feasible, but legally recognized

## Call to Actions regarding Digital Identity & GDPR:

The key call to actions from the discussion are:

- **Advocate for a relative standard of identifiability under GDPR:** Building on identity protocols like KERI, encourage the European Data Protection Board and national authorities to adopt contextual, risk-based interpretations of identifiability. Where processors (e.g., blockchain nodes) lack reasonable means to re-identify individuals, such as when processing non-personal Key Event Logs (KELs), such data should be treated as anonymous, thus falling outside the scope of GDPR. This interpretation aligns with recent CJEU rulings (e.g., *EDPS v. SRB*) and reduces unnecessary compliance burdens on decentralized infrastructure operators.

- **Standardize selective disclosure and revocation mechanisms:** Work through ISO/DIN and industry consortia to create technical and legal standards for identity operations that balance verifiability with privacy.

### 3. Digital Identity in AML/KYC

The final topic, presented by Mariana de la Roche W. (BlackVogel), examined the evolving role of digital identity in AML, Know Your Customer (KYC), and Travel Rule enforcement. The session highlighted the paradox at the heart of compliance-driven identity systems: while they promise greater transparency and security, they risk creating excessive surveillance, undermining privacy, and placing disproportionate burdens on both users and industry actors.

Participants explored how digital identity frameworks could support a more efficient and rights-preserving approach to compliance, particularly if implemented using decentralized architectures and cryptographic tools. The idea of "identity on demand" emerged as a key concept: rather than transmitting personal data with every transaction, users could present a verifiable credential that proves a KYC check was performed by a trusted third-party. Only in the event of a flagged transaction would further identity verification be triggered. This selective disclosure model would allow compliance officers to fulfill regulatory obligations without accessing full user profiles or storing sensitive data unnecessarily.

Nevertheless, the crypto industry has proactively developed innovative compliance-enhancing tools since its early days, not because of regulatory mandates, but because doing so was in the interest of users and market integrity. From selective disclosure to credential-based attestations, many solutions now exist that could help regulators meet their objectives without sacrificing privacy or inclusion.

Despite its promise, this approach currently faces legal and institutional barriers, especially within the EU. Under existing AML and GDPR frameworks, the reuse of KYC certificates and the non-sharing of personal data between entities may conflict with current interpretations of due diligence and supervisory access. Participants noted that in traditional finance, banks often rely on third-party KYC verifications without issue. Extending this logic to CASPs could yield significant privacy gains and reduce compliance costs, but would require regulatory clarification or reform.

There was a strong consensus that current AML rules are overengineered and inefficient. Participants cited empirical data and regulatory feedback indicating that the billions spent on AML compliance often yield minimal results. Many AML structures, it was argued, breed the very inefficiencies and inequalities they seek to prevent: smaller firms are priced out of compliance, while sophisticated actors circumvent controls with ease. In this context, digital identity frameworks risk becoming tools of exclusion or performative compliance, rather than meaningful safeguards.

To move forward, participants emphasized the importance of designing interoperable, risk-based systems that adapt verification requirements to transaction context and user risk profile. Credentials should be revocable, auditable, and compatible with GDPR. Authorities could confirm that obligations were fulfilled not through direct data access, but via cryptographic attestations or ZKP. This would reduce unnecessary data exposure while maintaining traceability.

The conversation also touched on the broader policy failure of siloed regulation: AML, data protection, and technological innovation have evolved in isolation, creating contradictory mandates. There was a call for greater coordination among regulators, as well as structured industry input, particularly through sandboxes and legislative feedback mechanisms.

Participants agreed that the aim is not to replace compliance with anonymity, but to realign it with proportionality, efficiency, and user agency. The industry must take the lead in proposing alternatives that respect rights without compromising on enforcement objectives.

| Call to Actions regarding AML/KYC and Digital Identity |
| --- |
| The key call to actions from the discussion are:<br>● **Pilot privacy-preserving KYC models based on reusable credentials and selective disclosure**, allowing compliance obligations to be fulfilled through verifiable attestations rather than bulk data collection.<br>● **Establish structured dialogue between regulators and industry innovators**,especially within EU innovation sandboxes, to test and co-design solutions that align AML enforcement with GDPR and fundamental rights. |

We thank all participants of the Berlin 5.0 DARTE event for contributing to the discussion:

Aiden Ward (Radix Foundation), Åsa Dahlborn (BlackVogel), Benedikt Faupel (Bitpanda), Benjamin Buergi (Cardano Foundation), Colin Nimsz (Brighter AI), Florian Daniel (Westernacher), Florian Reul (Schufa), Janine Roemer, Jannik Piepenburg (Deloitte), Joachim Schwerin (EU Commission), Jonas Hammer (IDUnion), Jörn Erbguth (Geneva Macro Labs), layer0 (Powerhouse), Maria Claudia Rodriguez (BlackVogel), Mariana de la Roche (BlackVogel), Martijn Keuzenkamp, Mathias Nörenberg (N26), Nicolas Jacquemart (Cardano Foundation), Nina-Luisa Siedler (siedler legal), Oliver Nägele (Blockchain Helix), Radoslav Albrecht (Bitbond), Silvan Jongerius (TechGDPR), Tamari Asatiani (BVR), Yannick Scholz (BaFin).)