The relevance of ISO TS 29496 to the European regulatory landscape for Distributed Ledger Technology

by Robin Renwick
(BlockSTAND expert)

[illegible]

Introduction

Distributed Ledger Technology (DLT), over the last decade, has embedded itself into mainstream culture. Bitcoin is a technology recognised across the world, with access now afforded through a host of applications, digital banking apps, wallets, as well as specific crypto-currency and DLT-related service providers.

In the last five years, the accessibility and perceived value of DLT-based projects has increased markedly, whether though the prism of Non-Fungible Tokens (NFTs), meme-coins, prediction markets, blockchain gaming and the meta-verse, and even the emergence of DLT-based 'AI agents'.

2024 saw rapid changes in both retail and, more importantly, institutional acceptance, exemplified best with the approval of Exchange Traded Funds (ETFs), that provide institutional investors a tightly regulated 'on-ramp' into the world of cryptocurrency investment.

While adoption strongly favours an upward trajectory, there are still aspects of the technology that remain uncertain. One of these is how the technology can reside peacefully alongside robust information technology (IT) concepts such as privacy and data protection.

Coupled to this, the international (and European) standardisation communities are recognising that the evolving regulatory landscape is putting pressure on the DLT ecosystem to provide harmonised solutions to problems explicitly driven by exacting legislative frameworks – whether in the realms of trust services and digital identity, cybersecurity and cybersecurity certification, anti-money laundering and counter-terrorist financing, digital privacy, and data protection.

This blog explores the emerging regulatory landscape through the lens of the European Market in Crypto-Assets Regulation (MiCAR)[1] and the Anti-Money Laundering Regulation (AMLR)[2] in Europe, and outlines the emerging tension between compliance requirements and privacy-preserving Distributed Ledger Technologies (DLTs)

Importance of privacy and data protection in Europe

1 http://data.europa.eu/eli/reg/2023/1114/2024-01-09
2 http://data.europa.eu/eli/reg/2024/1620/oj

Europe has always placed strong emphasis on the importance of privacy and data protection[3] – whether through the prism of economic and business value, consumer protection, or both concepts embedded relation to human rights.

The European community has enshrined both privacy and data protection into the European Charter for Fundamental Rights, through Articles 7 and Article 8, and the European Commission continually emphasises their importance, and position, in the continual digitalised evolution of European society, whether through the European Declaration of Digital Rights and Principles[4], or the Communication on the EU Data Strategy.[5]

Europe was the first continent to successfully enact a cross-border legislative framework for data protection (General Data Protection Regulation), which supplements the existing cross-border Directive for Electronic Privacy (e-Privacy Directive).

Both of these frameworks are seen as cornerstones of an open and free society. Stakeholders are legally obliged to respect and uphold critically important privacy and data protection rights through established rules, principles, and exacting compliance requirements enshrined in European, and Member State, privacy and data protection law.

Relation of privacy and data protection to the realm of standardisation

So what does all that background have to do with standardisation? How can the development of European or international standards, in Standards Development Organisations (SDOs) support the enactment of Fundamental Rights? The answer, while complex, is worth exploring.

To begin, the international standardisation community has always maintained a strong relationship with concepts such as privacy and data protection. Both concepts are viewed as integral components of, or explicitly related to, the concept of Information Technology (IT) security.

Security, from an IT perspective, has always been one of the most internationally appreciated realms of standardisation, with numerous SDO technical committees and working groups focusing explicitly on the topic.

At the International Organization for Standardization (ISO)[6], IT security focused working groups frame data protection (and the related protection of personal data) through the more internationally recognised concept of Personally Identifiable Information (PII). PII protection and security is the focus of a range of international standards, including security practices, governance, and certification.

At the ISO, there are specific technical committees tasked with the creation of standards to support the international harmonisation of IT security in relation to DLT. For example, “ISO/TC 307/JWG 4 - Security, privacy and identity for Blockchain and DLT" is a joint technical committee, housed within both “ISO/IEC Joint Technical Committee 1, Steering Committee 27 (JTC1/SC27) - Inform-

3 https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm
4 https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles
5 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066
6 https://www.iso.org/about

ation security, cybersecurity and privacy protection"[7] and "ISO Technical Committee 307 (TC307) - Blockchain and distributed ledger technologies".[8]

The joint nature of the working group allows experts from either technical committee to work on relevant projects, with expertise and knowledge being drawn from both. This collaborative approach fosters cross-fertilisation of ideas, and allows for the open exchange of technical expertise to enrich the standards that are being developed.

The state of DLT privacy and data protection

Since the birth of Bitcoin, and the subsequent development of the DLT ecosystem, it has become common knowledge that certain types of DLT implementations have consequences for information privacy and data protection.

Bitcoin, Ethereum, and a host of other public and permissionless implementations of the technology openly publish data on publicly accessible, distributed, ledgers. This is excellent for some IT characteristics such as audibility, verifiability, integrity and resilience, but not for others such as privacy and confidentiality.

While encryption and hashing mechanisms do provide a layer of privacy for DLT implementations, the vast majority of public and permissionless DLT systems maintain severe privacy risks related to the public and openly accessible nature of the data stored on them.

Previously, the ISO published a technical report "ISO/TR 23244:2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations"[9] which outlined current considerations for DLT systems from the perspective of privacy and data protection. Critically this project did not specify any guidance, or requirements, for capability assessment, technical improvement, or the preservation of privacy in DLT systems.

The scope of ISO TS 24946

"ISO 24946 Requirements and guidance for improving, preserving, and assessing the privacy capability of DLT systems"[10] is recently established project that will produce a technical specification. It is currently on its second Working Draft (WD). The project is housed within the previously mentioned JWG4 at the ISO. The project will develop an internationally harmonised specification for assessing, preserving, and improving the privacy capabilities of DLT systems.

It will outline an array of privacy related risks that DLT systems encounter, and provide meaningful DLT specific risk mitigation recommendations. The specification is of value to developers, operators, users, auditors, as well as regulators and policy makers who are evolving the DLT ecosystem internationally.

The importance of ISO TS 24946 and its relation to Europe

---

7 https://www.iso.org/committee/45306.html
8 https://www.iso.org/committee/6266604.html
9 https://www.iso.org/standard/75061.html
10 https://www.iso.org/standard/88614.html

An international DLT privacy specification, published by the ISO, will always be of benefit to the European community especially as privacy and the protection of data is paramount to digitalisation efforts in Europe. This is true of TS 24926, which has already received attention from the European standardisation community, through the European Committee for Standardization (CEN)[11], which is one of is one of the three European SDOs (together with CENELEC and ETSI). CEN hosts a Joint Technical Committee (JTC) that focuses on DLT.[12]

As it stands, there are two working groups within this technical committee: "CEN/CLC/JTC 19/WG 01 - Decentralised identity management" and "CEN/CLC/JTC 19/WG 2 - Environmental sustainability". There is also a proposal to create a third, led by the German standards authority (DIN), named "CEN/CLC JTC 19/WG 3 - Personal identifiable information (PII) in Blockchain and DLT".

This WG will harmonise (where possible) efforts at the international level with those in Europe, including potential adoption of ISO TS 24946. This parallel work at the international and European level support the DLT ecosystem's pursuit of robust privacy, and also work to provide clarity and transparency to the application of privacy preserving technologies within DLT.

DLT-related regulation and the need for standards

Currently, Europe is exerting regulatory pressure onto DLT systems through the enactment of two legal frameworks – the Market in Crypto-Assets Regulation (MiCAR)[13], and the new Anti-Money Laundering Regulation (AMLR)[14].

Both of these legislative frameworks have ramifications for DLT developers, issuers, operators, and crypto-asset service providers that interact with DLT projects that provide strong privacy-preserving guarantees.

Not only do they both restrict the ability for interaction with privacy-preserving projects, they impose restrictions without providing any mitigations, or solutions, for the privacy risks inherent in non privacy-preserving implementations of DLT.

Not only does this seem out of character for European digitalisation goals, but it also seems incongruent with data protection principles and overarching fundamental goals such as those detailed in Article 7 and Article 8 of the European Charter of Fundamental Rights.

MiCAR's role in the European regulatory space

In June 2023, the Market in Crypto-Assets (MiCAR) regulation came into force. The legislative framework included a phased introduction of compliance requirements, which ended on December 2024. The phased introduction allowed Crypto-Asset Service Providers (CASPs), DLT token (including stablecoin) issuers, and DLT operators some time to adjust to the requirements and prepare.

---

11 https://www.cencenelec.eu/about-cen/

12 https://standards.cencenelec.eu/dyn/www/f?p=205:29:0::::FSP_ORG_ID,FSP_LANG_ID:2702172,25&cs=16E2ADC46E2536C73D74C407A6FE4B3FD

13 http://data.europa.eu/eli/reg/2023/1114/2024-01-09

14 http://data.europa.eu/eli/reg/2024/1620/oj

MiCAR covers a wide range of compliance obligations, with specific focus on (MiCAR, Article 2):

- transparency and disclosure requirements for the issuance or offer to trading of crypto-assets;
- requirements for the authorisation, supervision, operation, organisation and governance of crypto-asset service providers, and issuers of tokens;
- requirements for the protection of holders of crypto-assets;
- requirements for the protection of clients of crypto-asset service providers;
- measures to prevent insider dealing, unlawful disclosure of inside information and market manipulation related to crypto-assets.

While many of the obligations are welcomed by the DLT ecosystem in Europe, there is one sub-clause within Article 76 which has ramifications for operational privacy, data protection, security, and consumer protection in the European DLT ecosystem, as it limits what types of assets can be offered to the public through licensed CASPs. Article 76(3) states:

Article 76

Operation of a trading platform for crypto-assets

> (3) "The operating rules of the trading platform for crypto-assets shall prevent the admission to trading of crypto-assets that have an inbuilt anonymisation function unless the holders of those crypto-assets and their transaction history can be identified by the crypto-asset service providers operating a trading platform for crypto-assets."

The first section of the compliance requirement is quite clear. A CASP should not allow trading of a DLT token without a Know Your Customer (KYC) process being completed, and the identity known of the user of the service provider's platform. The second part of the obligation is less clear – and seems to impact greatly on what types of privacy-preserving features can be built into DLT implementations.

Privacy-by-design features and privacy-enhancing technologies for DLT have, internationally, been recognised previously within "ISO/TR 23244:2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations"[15], but it is not clear how these technologies are compatible with the wording of MiCAR Article 76(3).

This tension has meant that DLT developers and token issuers face some uncertainty regarding which technologies are acceptable and which are not. The phrase "inbuilt anonymisation function" is also not well-defined, and the compliance requirement could easily be interpreted as meaning that all DLT transactions should be traceable (to an identity) and linkable (across transactions) – which would seem to be inconsistent with standard IT security and privacy recommendations. This seeming inconsistency is yet to be solved.

European Anti-Money Laundering Regulation

15 https://www.iso.org/standard/75061.html

Alongside MiCAR, the European Commission have published a new Anti-Money Laundering Regulation (AMLR). This piece of legislation (enacted in June 2024) is part of a legislative framework that will harmonise Anti-Money Laundering law across Europe.

The AMLR also targets certain privacy-enhancing technologies through the lens of "anonymity enhancing coins" (AMLR, Article 2(1)(25)), defined as:

> 'anonymity-enhancing coins' means crypto-assets that have built-in features designed to make crypto-asset transfer information anonymous, either systematically or optionally;

Further to this, Article 79 provides a compliance obligation:

> **Article 79**
> **Anonymous accounts and bearer shares and bearer share warrants**
>
> 1. Credit institutions, financial institutions and crypto-asset service providers shall be prohibited from keeping anonymous bank and payment accounts, anonymous passbooks, anonymous safe-deposit boxes or anonymous crypto-asset accounts as well as any account otherwise allowing for the anonymisation of the customer account holder or the anonymisation or increased obfuscation of transactions, including through anonymity-enhancing coins.

Most IT security experts will agree, that anonymity is extremely difficult to achieve, especially in a world in which data stores are public, permissionless, and immutable (key characteristics of many implementations of DLT.

Most security expert will also acknowledge in the realms of data privacy, protection of personal data, and the pursuit of PII protection - 'anonymity enhancing functions' (or anonymity enhancing technology) are of value and, arguably, essential to providing specific privacy guarantees. This is no different in the world of DLT.

Coupled to this, it is currently unclear what privacy, data protection, and security related technologies should be pursued by those in the DLT ecosystem if they wish to safeguard user privacy and provide mechanisms for strong data protection guarantees.

If DLT token issuers, operators, and users are faced with a legislative framework that forbids privacy-enhancing technologies that provide for improved anonymity, how exactly should they pursue privacy and data protection goals?

This is especially important in an environment where DLTs are deployed in an array of sectors, especially ones such as health, digital identity, data spaces, and metaverses, where privacy and data protection are viewed as critical components.

International standardisation goals and the role of ISO TS 24946

It should be acknowledged that “ISO 24946 Requirements and guidance for improving, preserving, and assessing the privacy capability of DLT systems” will not be a panacea for resolving the current tensions between regulatory frameworks and privacy-preserving and privacy-enhancing technologies. However, it might help to harmonise perspectives of which techniques are available to the DLT ecosystem, and what specific risks they mitigate.

Outlining privacy risks and mitigation techniques will also work to inform regulators, policy makers, and legal experts on the benefits of privacy-preserving techniques, and also provide information on the limits of those technologies from an anonymity perspective, which in turn will provide an evidence base on which to determine whether these “anonymity-enhancing functions” provide more benefit than risk to the DLT (and financial) ecosystem.

Conclusion

In a world where data is being collected, processed, and stored on distributed, public, permissionless, and immutable ledgers, it is inconceivable that the DLT community will not welcome clarity on privacy and data protection risks and mitigation methods. Pursuing application of these mitigation methods in the pursuit of stronger privacy and data protection guarantees for users should be welcomed, and not forbidden from a regulatory perspective.

ISO TS 24946 will be the first internationally recognised technical specification to provide specific mitigation guidance, and should be welcomed by the European privacy and data protection community as Europe pursues overarching goals for European digitalisation, sovereignty, and the EU data strategy, whilst respecting fundamental privacy and data protection rights.