European Blockchain Sandbox
Best practices report
2nd Cohort

Bird & Bird / OXYGY

European
Blockchain
Sandbox

Internal identification

Contract number: CNECT/2021/OP/0019
VIGIE number: CNECT-PN-2021-000018-EBP

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology
Directorate E — Future Networks
Unit E.3 — Next-Generation Internet

Contact: CNECT-E3@ec.europa.eu

European Commission

B-1049 Brussels

European Blockchain Sandbox

Best practices report

2nd Cohort

Directorate-General for Communications Networks, Content and Technology
2025 EN

EUROPE DIRECT is a service to help you find answers to your questions about the European Union

Freephone number (*):
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you)

LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the European Commission is not liable for any consequence stemming from the reuse of this publication. The Commission does not guarantee the accuracy of the data included in this study. More information on the European Union is available on the Internet (http://www.europa.eu).

PDF Web	ISBN 978-92-68-26348-8	doi: 10.2759/8586422	KK-01-25-034-EN-N

Manuscript completed in April 2025.

First edition

The European Commission is not liable for any consequence stemming from the reuse of this publication.

Luxembourg: Publications Office of the European Union, 2025

© European Union, 2025

The reuse policy of European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under a Creative Commons Attribution 4.0 International (CC-BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightholders.

Table of Contents

1. INTRODUCTION 2ND COHORT 9

1.1. OBJECTIVES AND POLICIES 9
1.2. SELECTED USE CASES, 2ND COHORT 11
1.3. OUTCOME OF THE MATCHING FOR THE 2ND COHORT 11
1.4. FORMAT OF THE 2ND COHORT REGULATORY DIALOGUES 12
1.5. FOCUS OF THE 2ND COHORT REGULATORY DIALOGUES 14
1.6. CONTENT OF THIS REPORT 14

2. TERMINOLOGY, RELEVANT LAWS AND REGULATIONS 16

2.1. TERMS, ABBREVIATIONS, AND LEGISLATION 16
2.2. BLOCKCHAIN AND DLT INFRASTRUCTURES 16
2.3. RELEVANT LAWS AND REGULATIONS FOR BLOCKCHAIN/DLT APPLICATIONS 17
2.4. LEGAL AND REGULATORY FOCUS AREAS FOR THE 2ND COHORT 18
2.5. LOOKING AHEAD: THE 3RD COHORT 20

3. DATA PROTECTION (GDPR) – REGULATORY COMPLIANCE 21

3.1. INTRODUCTION 21
3.2. KEY QUESTION: DOES THE DATA RECORDED ON THE LEDGER QUALIFY AS PERSONAL DATA? 22
3.3. APPLICATION OF THE GDPR IN THE CONTEXT OF PUBLIC PERMISSIONLESS BLOCKCHAINS 22
3.4. DATA PROTECTION ROLES 23
3.4.1. Qualification of the role of node operators in a public permissionless blockchain 24
3.4.2. The position of wallet providers 24
3.4.3. Best practice regarding data protection roles 24
3.5. LEGAL BASIS 24
3.6. GENERAL DATA PROCESSING PRINCIPLES (FOCUS ON DATA MINIMISATION, ACCURACY AND TRANSPARENCY) 26
3.7. DATA SUBJECT RIGHTS – RIGHT TO ERASURE 27
3.8. THE USE OF SMART CONTRACTS IN THE CONTEXT OF ARTICLE 22 GDPR 28
3.9. GDPR COMPLIANCE MEASURES IN THE EVENT OF INTEROPERABILITY BETWEEN DLT USE CASES 29
3.10. THE INTERSECTION OF THE GDPR AND OTHER AREAS OF LEGISLATION 30
3.11. TOPICS FOR FURTHER DISCUSSION IN THE 3RD ROUND OF EBS DIALOGUES 30

4. RELEVANCE OF THE EIDAS REGULATION FOR BLOCKCHAIN/DLT SOLUTIONS 31

4.1. INTRODUCTION TO THE EIDAS CHAPTER 31
4.2. RELEVANCE OF THE EIDAS REGULATORY FRAMEWORK FOR BLOCKCHAIN/DLT SOLUTIONS – GENERAL PERSPECTIVE 31
4.2.1. Introduction 31
4.2.2. Implementing Acts and the ARF 34
4.2.3. Standards 35
4.2.3.1. General – eIDAS standards and standardization initiatives (not exhaustive) 36
4.2.3.2. eIDAS standards and standardization initiatives focused on blockchain/DLT (not exhaustive) 36
4.2.3.3. Other eIDAS standards and standardization initiatives relevant for blockchain/DLT use cases (not exhaustive) 37
4.2.4. Best practices and lessons learned 38
4.2.4.1. Applicability of standards and harmonization 38
4.2.4.2. Use of blockchain/DLT solutions for trusted lists and registers of relying parties 38
4.2.4.3. Identification of relevant electronic identification means and trust services 39
4.2.5. Areas for further dialogue and clarification 41
4.3. INTERPLAY BETWEEN EIDAS & COMPANY DIRECTIVE – EU COMPANY CERTIFICATE AND DIGITAL EU POWER OF ATTORNEY 42
4.3.1. Introduction 42
4.3.2. Electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source 44
4.3.3. Best practices and lessons learned 45
4.4. INTERPLAY BETWEEN EIDAS & AML/KYC REQUIREMENTS IN THE AMLR 47
4.4.1. Introduction 47

4.4.2. Best practices and lessons learned ... 48
4.4.3. Areas for further dialogue and clarification ... 49
4.5. INTERPLAY BETWEEN EIDAS & IOT DEVICES ... 49
4.5.1. Wallets for objects such as IoT devices? ... 49
4.5.2. Relevant eIDAS 2 regulatory instruments for DLT/IoT solutions ... 50
4.5.3. Areas for further discussion: ... 50

5. BLOCKCHAIN/DLT AND AI ... 51

5.1. INTRODUCTION ... 51
5.2. COMBINATION OF TECHNOLOGIES: DLT/BLOCKCHAIN AND AI ... 53
5.3. REGULATION OF OPEN SOURCE AI SYSTEMS AND AI PRODUCTS IN THE AI ACT ... 54
5.4. AREAS FOR FURTHER CLARIFICATION & DIALOGUE ... 55
5.4.1. Areas for deeper dives ... 55
5.4.2. Additional topics ... 56

6. DECENTRALISED AUTONOMOUS ORGANISATIONS (DAOS) – LEGAL WRAPPER; GDPR COMPLIANCE ... 57

6.1. INTRODUCTION ... 57
6.2. LEGAL ENTITY STATUS ... 58
6.3. CASE STUDY - CAN DAO CHARACTERISTICS BE FACILITATED BY AN SCE? ... 59
6.4. GDPR COMPLIANCE IN THE CONTEXT OF A DAO ... 60
6.5. AREAS FOR FURTHER CLARIFICATION & DIALOGUE TOPICS FOR THE NEXT COHORTS ... 61

7. BLOCKCHAIN/DLT SOLUTIONS FOR E-VOTING ... 63

7.1. INTRODUCTION ... 63
7.2. E-VOTING: REGULATORY FRAMEWORK E-VOTING AT EU LEVEL ... 63
7.3. E-VOTING: FORMAL ELECTIONS, REFERENDUMS, CONSULTATION PROCESSES ... 64
7.4. E-VOTING: REGULATORY FRAMEWORK AND DLT BASED E-VOTING USE CASES AT NATIONAL LEVEL ... 65
7.4.1. Greece ... 65
7.4.2. Estonia ... 65
7.4.3. Romania ... 66
7.5. RELEVANCE OF EIDAS 2 REGULATORY INSTRUMENTS FOR (DLT BASED) E-VOTING APPLICATIONS IN ELECTIONS ... 67

8. BLOCKCHAIN/DLT SOLUTIONS ENHANCING CSRD COMPLIANCE ... 68

8.1. GENERAL FRAMEWORK ... 68
8.1.1. CSRD ... 68
8.1.2. ESRS ... 69
8.1.3. Regulatory Update February-April 2025 ... 70
8.1.4. The Sustainability statement ... 70
8.1.5. Appointment and the role of national competent authorities ... 72
8.2. BEST PRACTICES, LESSONS LEARNED ... 72
8.2.1. Key question: to what extent can DLT/blockchain solutions enhance compliance with CSRD reporting obligations? ... 72
8.2.2. Guidance to national competent authorities ... 72
8.2.3. Areas for further clarification & dialogue topics for the next cohorts ... 74

9. BLOCKCHAIN/DLT SOLUTIONS ENHANCING COMPLIANCE WITH THE EUDR AND THE INTERPLAY WITH HORIZONTAL DATA REGULATION ... 75

9.1. INTRODUCTION – THE EU DEFORESTATION REGULATION (EUDR) ... 75
9.2. INTERPLAY WITH THE UN TRANSPARENCY PROTOCOL AND RECOMMENDATION 49 ... 76
9.3. INTERPLAY BETWEEN THE EUDR AND HORIZONTAL EU DATA REGULATION ... 77
9.4. STANDARDISATION AND INTEROPERABILITY IN THE GREEN DEAL DATA SPACE, INCLUDING THE EUDR ... 77
9.5. DATA ACT - QUALIFICATION OF BLOCKCHAIN/DLT APPLICATIONS FOR ESG MONITORING AND REPORTING AS "DATA PROCESSING SERVICES"? ... 78
9.6. RELEVANCE OF THE DGA AND THE DSA? ... 79

10. BLOCKCHAIN/DLT SOLUTIONS FOR BATTERY PASSPORTS AND DPP'S AND THE INTERPLAY WITH HORIZONTAL DATA REGULATION ... 81

10.1. INTRODUCTION ... 81

10.2. Blockchain/DLT solutions for Battery Passports and DPPs under the Battery Regulation and the ESPR .. 82
10.3. Status Update on Implementing Acts, Standards, and Interoperability Provisions for Battery Passports/DPPs since the 1st best practices report 82
10.4. Data Deletion Requests / Continuity 84
10.5. Interplay between the Battery Regulation/ESPR and the Data Act 84
10.5.1. Battery Regulation/ESPR 84
10.5.2. Data Act 85
10.6. Relevance of the DGA and the DSA? 86

11. COMPLIANCE WITH THE DATA GOVERNANCE ACT AND THE DIGITAL SERVICE ACT 87

11.1. Applicability of the DGA to Blockchain/DLT solutions? 87
11.2. Applicability of the DSA – Qualification of Blockchain/DLT solutions as "intermediary service" 89
11.3. Areas for further clarification & dialogue topics for the next cohorts 90

12. BLOCKCHAIN/DLT SOLUTIONS TO ENHANCE COMPLIANCE WITH SANCTIONS LISTS 91

12.1. Introduction 91
12.2. Best practices and lessons learned 91

13. BLOCKCHAIN/DLT SOLUTIONS TO ENHANCE AML COMPLIANCE 93

13.1. Introduction 93
13.2. Outsourcing/third party service provision of AML regulatory requirements 95
13.3. Applicability of the Transfer of Funds Regulation to e-money tokens 97
13.4. Areas for further clarification and dialogue 97

14. DORA - REGULATORY COMPLIANCE 99

14.1. Introduction 99
14.2. Key Question: To what extent are DORA regulatory requirements relevant for DLT/Blockchain solution providers? 99
14.2.1. Direct relevance of DORA for DLT/Blockchain providers which qualify as "financial entities" . 99
14.2.2. Indirect relevance of DORA for DLT/Blockchain solution providers that qualify as "ICT third-party service provider" 100
14.3. Best practices and lessons learned 102
14.3.1. Qualification of Blockchain/DLT solutions as ICT third-party service providers - supporting critical or important functions? 102
14.3.2. Smart contracts will normally qualify as "ICT asset" 102
14.3.3. Standards for smart contracts 103
14.3.4. Requirements for testers for carrying out TLPT 104
14.4. Areas for Further Clarification & Dialogue Topics for the Next Cohorts 105

15. SCOPE AND DELINEATION MIFID & MICAR 106

15.1. Introduction 106
15.2. National corporate law aspects on tokenization of shares and qualification of tokenized assets 107
15.3. Step-by-step analysis for the classification of tokenized instruments 108
15.4. Areas for further clarification and dialogue 109

16. USE OF THE DLT PILOT REGIME 110

16.1. Introduction 110
16.2. Application for DLT Pilot Regime exemptions 111
16.3. Outsourcing of services by a DLT SS/DLT TSS provider as part of an application for a DLTPR exemption ... 113
16.4. Areas for further clarification & dialogue 113

17. COMPLIANCE WITH MICAR 115

17.1. Introduction 115
17.2. MiCAR – regulatory framework 115
17.3. Transferability – best practices and lessons learned 116
17.4. Non-uniqueness and Fungibility – best practices and lessons learned 117
17.5. Applicability of MiCAR – who is the issuer? 117

17.6. Exemptions from certain MiCAR requirements – best practices and lessons learned 118
17.7. Regulated/unregulated custody – best practices and lessons learned 119
17.8. Gas/transaction fees 119
17.9. Applicability of PSD2 and EMD2 or MiCAR 120
17.10. Areas for further clarification & dialogue 122

18. APPLICATION OF THE ECSPR 123

18.1. Introduction 123
18.2. Capital requirements - cumulative thresholds 123
18.3. Crowdfunding and custody 124
18.4. Areas for further clarification & dialogue topics for the next cohort 125

19. AUTOMATED MARKET MAKERS & LIQUIDITY POOLS 127

19.1. Introduction Automated Market Makers 127
19.2. Automated Market Makers for financial instruments 127

20. CONCLUSIONS AND NEXT STEPS 129

21. LIST OF ABBREVIATIONS 132

22. TERMS AND DEFINITIONS 134

22.1. Terms used in the Report 134
22.2. Common short forms of EU legislation 135

23. ANNEXES 140

23.1. Use cases 2nd Cohort 140
23.2. Annex to Chapter 5 (AI Act) – Overview of legal obilgations to offering* AI Systems, tools, services, components, or processes (jointly referred to as "AI products") that are provided "under free and open source licences" 141
23.3. Annex to Chapter 6 (DAO's) - Case study - Can DAO characteristics be facilitated by an SCE? 142

1. Introduction 2nd cohort

1.1. Objectives and policies

This best practices report presents the lessons learned, best practices and recommendations that were identified during regulatory dialogues that were held as part of the 2nd round of the European Blockchain Sandbox. The results of the 1st round of the European Blockchain Sandbox were published in June 2024. The reguatory dialogues for the 3rd and final round of the European Blockchain Sandbox are ongoing and the results are expected to be published by the end of 2025.

The *European Blockchain Sandbox* is a regulatory sandbox which aims to establish a pan-European framework for regulatory dialogue. This initiative of the European Commission brings together national and EU regulators and authorities with providers of innovative blockchain/DLT applications in both the private and public sector to identify possible issues and solutions from a legal & regulatory perspective in a safe and confidential environment.

The cross-border regulatory dialogues will allow innovators to better understand relevant laws and regulations. The exchanges will allow regulators and authorities to enhance their knowledge of cutting-edge technologies involving blockchain and distributed ledger technologies, and to exchange views and experiences with other regulators and authorities.

The European Blockchain Sandbox does not imply legal endorsement or regulatory approval of the use cases, nor does it allow for derogations of applicable laws. Results are made available to the wider community through best practice reports.

The initiative annually supports 20 projects and has started in 2023. The sandbox is open to use cases based on any blockchain infrastructure. Blockchain/DLT use cases are selected on the basis of published eligibility and award criteria and matched with relevant regulators and supervising authorities. Blockchain/DLT applications that are based on a combination with other innovative technologies such as AI and IoT are becoming more relevant every year.

The sandbox is funded under the Digital Europe Programme and delivers on the Commission Communication “SME” of 10 March 2020[1] and “A European Strategy for Data” of 19 February 2020.[2] Funded by the Digital Europe Programme and delivering on the SME strategy, the sandbox runs from 2023 to 2026 and will annually support 20 projects including public sector use cases on the European Blockchain Services Infrastructure. Projects are chosen through calls for expression of interest. After the dialogues for each cohort, the most innovative regulator participating in the sandbox will be awarded a non-monitory prize.

The European Blockchain Sandbox is facilitated by a consortium under the leadership of the law firm Bird & Bird and its consulting arm OXYGY supported by blockchain experts of Warren Brandeis, local regulatory experts in all EEA Member States and web-designers of Spindox, which has been procured through an open call for tenders in 2022. The selection process for each cohort is overseen by a panel of independent academic experts consisting of Professor Roman Beck (IT-University, Copenhagen (until December 2024) and Bentley University (Boston, US) since January 2025),, Professor Soulla Louca (University of Nicosia, Cyprus) and Professor Walter Blocher (University of Kassel).

1 An SME Strategy for a sustainable and digital Europe COM (2020) 103 (10 March 2020).
2 A European strategy for data COM(2020) 66 (19 Feb. 2020).

The sandbox is a contribution to responding to the call for action in the Council Conclusions from November 16, 2020,[3] where it stipulates as follows:

> *Regarding regulatory sandboxes: CALLS on the Commission to organise, in cooperation with Member States, an exchange of information and good practices regarding regulatory sandboxes between Member States and itself in order to:*
>
> *a) establish an overview of the state of play regarding the use of regulatory sandboxes in the EU;*
>
> *b) identify experiences regarding the legal basis, implementation and evaluation of regulatory sandboxes;*
>
> *c) analyse how learning from regulatory sandboxes at national level can contribute to evidence-based policy making at EU-level.*

The pan-European blockchain regulatory sandbox and other EU initiatives such as the European Forum for Innovation Facilitators ("**EFIF"**)[4] for Digital Finance and the sandboxes that have to be established at national level on the basis of the AI Act and should be operational by 2 August 2026[5] are complementary and reinforce each other. The European blockchain regulatory sandbox provides a framework for a cross-border regulatory dialogue with a focus on innovative blockchain applications across industry sectors covering a broad range of regulatory and potential legal issues, while the AI Regulatory Sandboxes to be established across the EU under the AI Act will be specialized on AI to foster innovation and provide a controlled regulatory environment for the development, validation and testing of innovative AI systems, including where relevant in real-world conditions, under the guidance and supervision by competent authorities under the AI Act. The European Forum for Innovation Facilitators (EFIF) is the platform for EU financial supervisors to meet regularly and share experiences from engagement with firms through "innovation facilitators" (a catch-all term for regulatory sandboxes and innovation hubs). The objectives are to share technological expertise, reach common views on the regulatory treatment of innovative products, services and business models, and encourage bilateral and multilateral coordination on sandbox testing where relevant..[6] Blockchain use cases that have been onboarded through the European blockchain regulatory sandbox can be connected with relevant financial supervisors through EFIF in pertinent use cases. Given the increasing convergence of innovative technologies in use cases often involving several industry sectors, there is a close collaboration between the European Blockchain Sandbox and these other initiatives on EU and national level to make sure that experiences and insights are shared and synergies are leveraged.

Moreover, the pan-European blockchain regulatory sandbox is an integral part of the European Commission's blockchain strategy.[7]

---

3 Council Conclusions on Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age, 13026/20 BETREG 27 (16 November 2020).

4 European Forum for Innovation Facilitators | EU Digital Finance Platform (europa.eu).

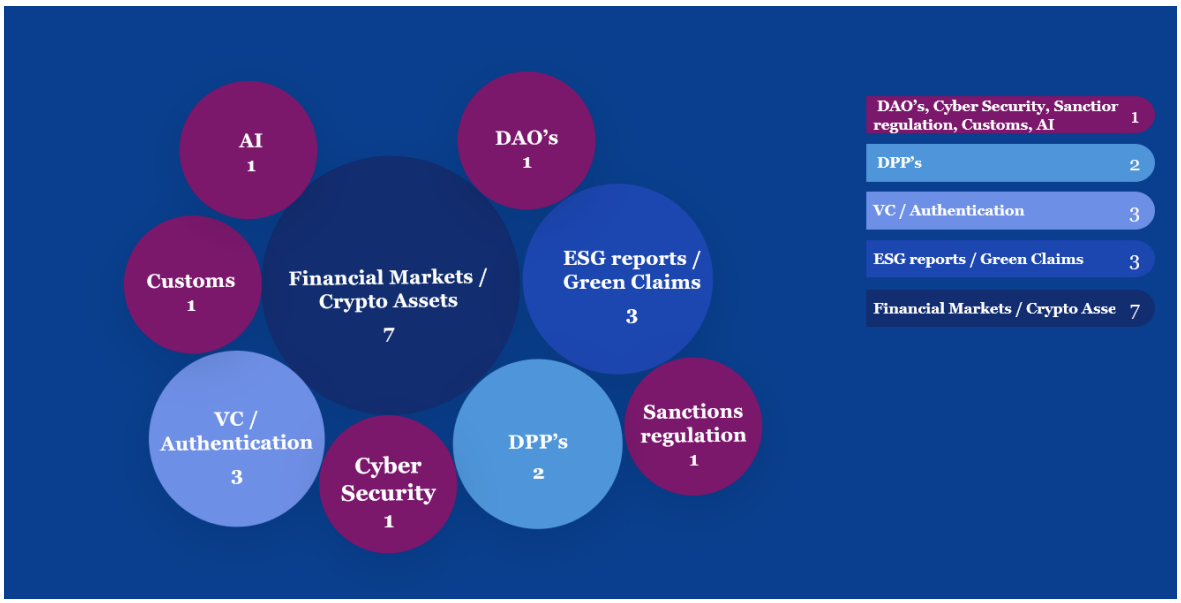
5 Chapter VI, Articles 57 – 59 AI Act (Regulation (EU) 2024/1689 (Artificial Intelligence Act).

6 European Forum for Innovation Facilitators | EU Digital Finance Platform (europa.eu) with a reference to the Joint ESA report on regulatory sandboxes and innovation hubs; see page 5: "Regulatory sandboxes: these provide a scheme to enable firms to test, pursuant to a specific testing plan agreed and monitored by a dedicated function of the competent authority, innovative financial products, financial services or business models. Sandboxes may also imply the use of legally provided discretions by the relevant supervisor (with use depending on the relevant applicable EU and national law) but sandboxes do not entail the disapplication of regulatory requirements that must be applied as a result of EU law."

7 Blockchain Strategy | Shaping Europe's digital future (europa.eu).

1.2. Selected use cases, 2nd cohort

After the launch of the 2nd round of applications on 25 January 2024, the European Blockchain Sandbox has gone through a successful second application round, which after a rigorous selection process resulted in an impressive 2nd cohort of 20 innovative blockchain/DLT use cases which were announced in June 2024.[8]



The 2nd cohort of selected use cases (including one EBSI use case) represents between them all EU/EEA regions and a range of industry sectors. As in the 1st cohort, the financial/crypto asset applications are again well represented but not dominating, and a broad variety of other use cases is represented in the 2nd cohort, covering areas such as AI, verifiable credentials/authentication, ESG reporting, digital product passports, e-voting, customs, cyber security, data sharing and DAOs and combinations with other innovative technologies such as AI and IoT. The 2nd cohort selected use cases are included in **Annex I** to this report.

1.3. Outcome of the matching for the 2nd cohort

The European Blockchain Sandbox attracted again significant interest among national and EU regulators/authorities. The use cases in the 2nd cohort have been successfully matched with well over 80 national and EU regulators/authorities from across the EU/EEA and covering a broad range of regulatory areas.[9]

On average, approximately 8 regulators/authorities have participated in the 1st cohort cross-border dialogues for each individual use case (exceeding the initial objective of an average of 1.5 regulators per use case and exceeding the average of approximately 4 regulators/authorities in the 1st cohort). Financial market authorities competent for financial sector regulation, MiCAR and AML were again well represented in the dialogues for the 2nd cohort, which is important in view of the number of financial sector use cases in the 2nd cohort and the broad range of relevant regulatory areas within the competences of the financial sector authorities.

8 European Blockchain Sandbox announces the selected projects for the second cohort - European Commission.

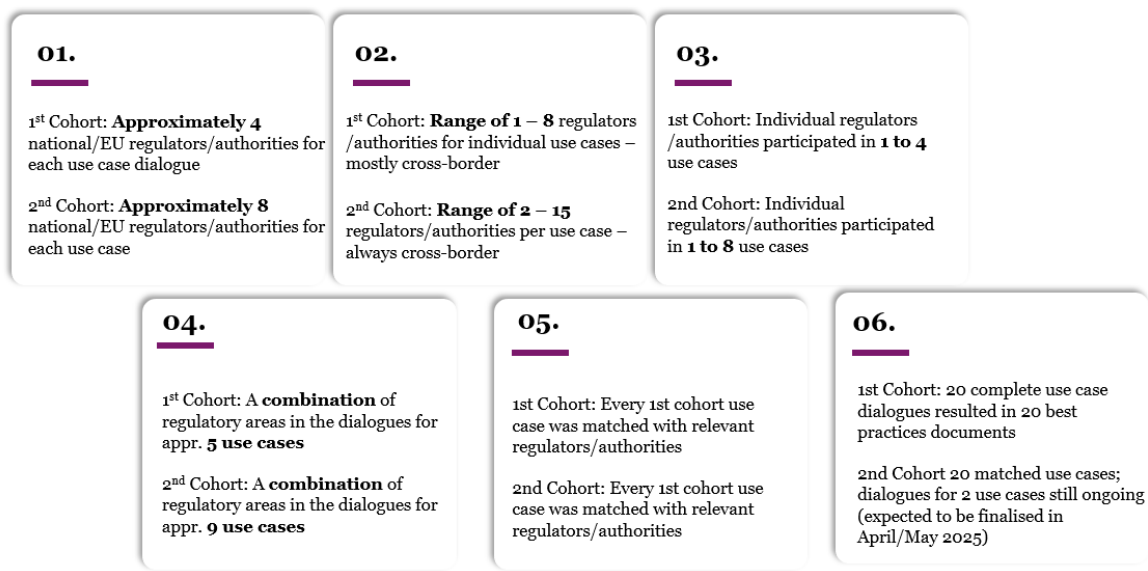
9 In comparison: more than 50 national and EU regulators participated in the 1st round of dialogues.

An overview of participating regulators/authorities is published on the project website (European Blockchain Sandbox Announces the regulators/authorities in the second cohort - European Commission.

The dialogues for all 2nd cohort use cases were cross-border with a range from 2 to 15 national and EU regulators/authorities per use case. A combination of national and EU regulators participated in the dialogues for nine of the 2nd cohort use cases. Many regulators /authorities participated in more than 1 use case with a range from 1 to 8 use cases. The regulatory dialogues for 9 use cases focussed on more than 1 regulatory area such as the GDPR and AML, eIDAS and AML, eIDAS and the Company Directive, eIDAS and e-voting, DPP's and data regulation and the EUDR and data regulation.

At the end of the matching process every 2nd cohort use case was matched with relevant regulators/authorities.

A comparision on the basis of some of the key indicators for the 1st and the 2nd cohort is included in the overview below.



1.4. Format of the 2nd cohort regulatory dialogues

The dialogues for the 2nd cohort were organized in accordance with the project's Protocol for Sandbox Participation.[10] The regulatory focus areas and regulatory topics for the dialogues were determined based on the selected use cases and in consultation with the selected use case owners while taking into account the topics identified for further dialogue at the end of the 1st cohort and an appropriate balance of relevant regulatory areas for the 2nd round of dialogues. All participants were given access to a recorded 15-minute onboarding webinar.

In preparation of the dialogue meetings, participating regulators/authorities could join a one-hour blockchain expert session. These sessions were scheduled twice, before the start of the 2nd cohort dialogues for the first group of use cases and after a few months before the start of the dialogues for the remaining use cases. These blockchain expert sessions were provided by experts from Warren Brandeis and covered blockchain infrastructure and applications in

[10] This Protocol (version 2.0) can be accessed through the following hyperlink: a2960d26-9320-46f5-8275-79a3342bed5c_en

general. Following feedback after the 1st cohort of dialogues the blockchain expert sessions were no longer organised on a per use case basis.

The basic format for the dialogues consisted of two online dialogue meetings of each 1.5 hours. For each of the use cases, the first dialogue meeting started with a presentation by the use case owner followed by a Q&A. The first dialogue meeting also served as a stepping stone for the second dialogue meeting: based on the dialogue in the first meeting the agenda could be adjusted, additional participants could be invited and further information could be shared.

For a number of use cases, in particular in the financial sector, a regulator-only meeting was held between the 1st and the 2nd dialogue meeting and moderated by Bird & Bird experts. The regulator-only meeting between the 1st and the 2nd dialogue meeting was introduced following feedback after the 1st cohort of dialogues and allowed the participating regulators/authorities to reflect on the use case presentation, to formulate additional questions for the use case team and to exchange initial observations in preparation of the 2nd dialogue meeting with the use case team. The questions that were raised and the initial findings that were exchanged during the regulator-only meeting were shared with the use case team and answers/further observations could be shared in preparation of the 2nd dialogue meeting.

For some use case dialogues an additional dialogue meeting or final dialogue call was scheduled in consultation with the participants to properly complete the regulatory dialogue.

Regulatory experts from Bird & Bird have taken the lead in preparing the agenda for the dialogue meetings, taking on board suggestions and information from the use case owners and the participating regulators/authorities.

To ensure an efficient use of time, information about the use case and the agenda for the dialogue meetings with relevant legal/regulatory context and further relevant information as appropriate were made available on the secure platform in advance of every dialogue meeting. Depending on the use case and the regulatory area(s) as well as the competences and expertise of the participating regulators/authorities, the roles of the regulators/authorities ranged from very active preparation/participation to a semi-observer role.

Summaries of the discussions during the dialogue meetings were shared in draft with the participants to the individual dialogues after each meeting.

Following the dialogue meetings, a draft best practices document was prepared by Bird & Bird with proposed draft lessons learned, best practices and recommendations to be considered for the best practices report for review by the participants to the dialogue. The draft documents were adjusted on the basis of the comments submitted by the participants and semi-final versions were shared for final comments following which the best practices documents for every use case were finalised. If any of the participants had any reservations in relation to any of the elements proposed in the draft best practices document, such element would not become part of the best practices report.

Participants were requested to provide feedback by submitting a feedback form via EUSurvey. In the feedback form, the participants (both the use case owners and the regulators/authorities) were asked if participation in the European Blockchain Sandbox dialogues has met their expectations from a content and a time commitment perspective and how they would rate the dialogue meetings. In addition, the participants were requested to share any recommendation for additional regulatory topics for future dialogues and if they have any suggestions for improvement of the dialogues in the next cohort.

Feedback from the 2nd cohort selected use cases and the participating regulators/authorities is again very positive. The use cases appreciate the legal/regulatory guidance and the possibility to have an open dialogue with regulators/authorities. The regulators/authorities

appreciate to learn more about innovative use cases and to have a cross-border dialogue with other national and EU regulators/authorities.

The adjustments in the format of the dialogues that have been implemented following feedback after the 1st round of dialogues (blockchain expert sessions no longer per use case and a separate regulator-only meeting between the 1st and the 2nd dialogue meeting) were very well received and will therefore be continued in the 3rd round of dialogues.

1.5. Focus of the 2nd cohort regulatory dialogues

The focus of the regulatory dialogues depended on the use case and the regulatory area. As in the 1st round of dialogues there were three main approaches:

- Several dialogues focused on **regulatory compliance** by DLT/Blockchain use cases. Examples are the dialogues with a focus on the GDPR, the AI Act, Data Regulation, Sanctions Lists, AML, MiCAR and financial sector regulation. During these dialogues valuable guidance was provided by the participating regulators/authorities to the use cases which resulted in best practices and lessons learned which are presented in this best practices report. These best practices and lessons learned are presented on a generic level and are not specifically linked to individual use cases or dialogues. In view of the ongoing regulatory developments in each of these areas, these will likely again become relevant topics in the 3rd round of dialogues.
- Other dialogues focused on how the use DLT/Blockchain applications can **support efficient and effective compliance and oversight**. Examples of the use of Blockchain/DLT applications as an extra tool, making compliance and oversight more efficient, were discussed in connection with the AI Act, Battery Passports/DPPs, the EUDR and the CSRD. The use of Blockchain/DLT as part of mandatory monitoring, reporting and oversight will likely again become a relevant area for the dialogues in the next cohorts.
- Finally the use of new areas of regulation and existing or new regulatory tools and qualifications with a focus on **regulation as a facilitator** were discussed in some of the dialogues, such as (i) the use of legal wrappers for DAOs, (ii) the use of the EUDI Wallet and new categories of qualified trust services in scope of the eIDAS 2 Regulation, (iii) the introduction of the EU Corporate Certificate and the Digital EU Power of Attorney in the latest amendment of the Company Directive, (iv) the possibility to qualify as a recognized Data Intermediation Service in the sense of the Data Governance Act and the use of EU harmonized regulatory instruments such a MiCAR and the DLT Pilot Regime.

1.6. Content of this report

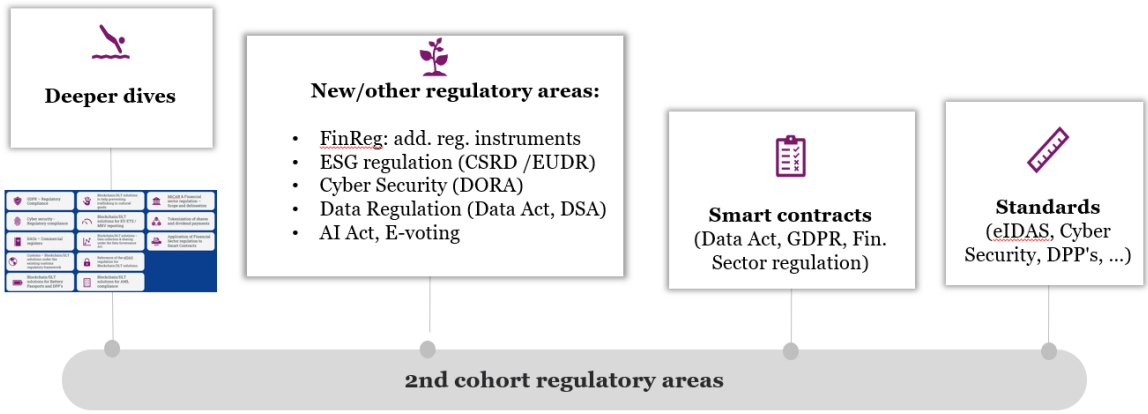
The combined final best practices documents for the 2nd round of dialogues have resulted in important lessons learned, best practices and recommendations which are presented in this 2nd cohort best practices report.

The 2nd cohort of selected use cases provided a basis for regulatory dialogues in areas that could not be covered in the 1st round such as the AI Act, e-voting, the EUDR, the Data Act and the Digital Services Act, DORA and new areas of financial sector regulation including the ECSPR. Some of the selected 2nd cohort use cases are based on a combination of technologies such as DLT/Blockchain in combination with AI and IoT which also triggered novel regulatory issues, for instance in the area of the AI Act and eIDAS.

Section 2 of this report discusses Blockchain/DLT Terminology and the relevant laws and regulations for Blockchain/DLT applications in general and more in particular for the 2nd cohort. The best practices and lessons learned for the 17 focus areas for the 1st cohort dialogues are presented in Sections 3 to 19. The conclusions and next steps are discussed in Section 20.

This 2nd cohort best practices report builds on the best practices, lessons learned, recommendations and topics for further regulatory dialogue that were identified in the 1st round of dialogues and are published as the best practices report, *1st cohort, Part B* (Best practices report 2023 - Part B - European Commission).[11]

In the individuel chapters of this 2nd cohort best practices report, references are made to the relevant chapters in the 1st cohort best practices report. Such references and quotations are presented in *blue*. The visual below provides a summary of the main regulatory areas for the 2nd round of dialogues. **The manuscript for this report was completed on 4th of April 2025.**



[11] The setting up of the European Blockchain Sandbox, the application & selection process and the matching with relevant regulators and supervising authorities for the first cohort of 20 uses cases is published as the best practices report, 1st cohort, Part A (link).

2. Terminology, relevant laws and regulations

2.1. Terms, abbreviations, and legislation

A list of terms, abbreviations and (abbreviations of) legislation is included at the end of this best practices report (22) . This list has been updated compared to the 1st cohort best practices report.

2.2. Blockchain and DLT infrastructures

The EU has the ambition to be a leader in blockchain and web3 technology, becoming a major innovator in blockchain and a home to significant platforms, applications, and companies. Reference is made to the Blockchain and Web3 Strategy which is published here: https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy:

> *Blockchain/web3 technology allows people and organisations who may not know or trust each other to collectively agree on and permanently record information without a third-party authority. By creating trust in data in ways that were not possible before, blockchain has the potential to revolutionise how we share information and carry out transactions online.*
>
> *The Commission's strategy supports the use and the development of key areas of blockchain/web3 in adherence to European values and regulations:*
>
> - ***Enhanced trust services**: Blockchain solutions provide a high level of trust and are being used in many pilot/deployment projects, policy actions, and R&D investments are being made in sectors like climate, energy, mobility, and agriculture.*
> - ***Environmental sustainability**: Blockchain technology should be sustainable and energy efficient.*
> - ***Data protection**: Blockchain technology should ensure compliance with the EU's strong data protection and privacy regulations.*
> - ***Digital Identity**: Blockchain technology aims to enhance evolving digital identity frameworks for persons, organisations, and items. It can contribute to the implementation of the EUDI framework and support other relevant authentication purposes.*
> - ***Cybersecurity**: Blockchain technology can provide high levels of cybersecurity.*
> - ***Interoperability**: For blockchains and Web3 to succeed, they need to be interoperable with each other and with other existing systems.*

Despite its name, the European Blockchain Sandbox is not only open for blockchain use cases but for all Distributed Ledger Technology ("DLT") use cases. The terminology in relation to DLT infrastructures and use cases is not always applied in a consistent manner. In this report we will use the terminology and definitions in the DLT specific legal instruments such as the DLT Pilot Regulation and the MiCAR as a starting point.

DLT or blockchain applications can be deployed either stand-alone or in combination with other innovative technologies (e.g. ICT services, cloud services, big data, AI, IoT, quantum computing, etc.). Blockchain is one type of a distributed ledger which organizes data into blocks, which are chained together in an append only mode.

Blockchains and other DLT infrastructures can be private or public and permissioned or permissionless. The terms public/private refer to who has read-write access to the chain; a public blockchain can be accessed by anyone and in a private blockchain access is limited. The second distinction, permissioned/permissionless, refers to the nodes in the network that validate updates to the ledger. In a permissionless blockchain anyone can be a node in the

network and validate updates while in a permissioned blockchain this is restricted to a specific group. Private-permissioned blockchains are mainly found in consortia of companies that all know each other and where transactions are mostly limited to the group of companies participating in the consortium such as a trading system within a specific industry.

The consensus mechanism consists of the rules and procedures by which an agreement is reached, among DLT network nodes, that a transaction is validated.[12] Blockchain and distributed ledger technology use cases often operate on the basis of smart contracts meaning a computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering.[13]

Blockchain technology is therefore not a one size fits all. The characteristics of the blockchain infrastructure and technical standards, the data flows and the use cases are important to understand the regulatory issues.

2.3. Relevant laws and regulations for Blockchain/DLT applications

A broad range of EU and national laws and regulations can be relevant to individual blockchain/DLT use cases. Many of these laws and regulations are in the process of development or under review or have been adopted very recently. Moreover, existing laws and regulations have to be applied in a decentralised context, often in combination with other innovative technologies, which incurs new regulatory questions as well.

At the start of the project, the (proposed) areas of regulation and (proposed) DLT specific regulations were identified that could become relevant for the regulatory dialogues depending on the selected use cases. This list is updated as the project evolves and new innovative blockchain/DLT use cases are selected and participating in the dialogues. The table below is not exhaustive.

Generic relevant regulatory areas	Sector specific relevant regulatory areas	DLT specific regulations
• AI Act • AML/KYC • Battery Regulation • Cyber security • Consumer protection • Customs • Data Act • Digital Services Act • Data Governance Act • DAOs - Commercial registers • eIDAS 2 • EU ETS / MRV	• Automotive • Crypto assets • Cultural assets • Cyber secutiry (DORA) • Energy & Utilities • Education • Financial sector • Government • Health • Media • Retail • Trade & logistics	• MiCA Regulation • DLT pilot Regulation • Regulation on information accompanying transfers of funds and certain crypto-assets • Provisions in the Data Act • Provisions in eIDAS 2

[12] Article 2(3) DLT-pilot Regime and Article 3(3) MiCA.
[13] Article 2(39) of Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 (**Data Act**).

• GDPR • ESPR • Environmental, Social & Governance (ESG) regulation • Sanctions lists	• E-voting • EUDR	

Table 1: Relevant regulatory areas and DLT specific regulations (not exhaustive). A more elaborate list of relevant EU legislation is included at the end of this best practices report (Chapter 22.2).

2.4. Legal and regulatory focus areas for the 2nd cohort

The legal and regulatory focus areas for the 2nd round of dialogues have been determined on the basis of an analysis of each of the selected 2nd cohort use cases and in consultation with the use case owners bearing in mind the balance of regulatory areas/topics for discussion across the cohort. These regulatory areas are set out in the table below. The number correspond to the chapters in this best practices report.

Smart contracts and standards (including the interplay between the two) were important topics in many of the 2nd cohort dialogues in connection with different regulatory areas such as the GDPR, eIDAS, the AI Act, Battery Passports/DPP's, the CSRD, DAO's, the Data Act, DORA, the EUDR, e-voting and the application of financial sector regulation (including MiCAR).[14]

Chapters 2nd cohort best practices report	**Relevant (proposed) EU legislation per regulatory area[15]** ***[References to the 1st cohort best practices report are printed in italics]***
3. GDPR - Regulatory compliance	The GDPR *[Chapter 3, 1st cohort best practices report]*
4. Relevance of the eIDAS regulation for Blockchain/DLT solutions	eIDAS 2 Regulation *[Chapter 11, 1st cohort best practices report]*
5. Blockchain/DLT and AI	The AI Act *[Not covered in the 1st cohort best practices report]*
6. DAOs – Legal wrapper; GDPR compliance	EU Company Law[16] including the Company Law Directive, the Shareholders Rights Directive, the Register Interconnection Regulation and the Digital Company Law Directive, EEIG Regulation. SCE Regulation, SE Regulation, Proposed Directive for ECBAs *[Chapters 3 and 5, 1st cohort best practices report]*

[14] See also the Draft working document of ETSI which is currently work in progress "Electronic Signatures and Trust Infrastructures (ESI); Standardisation requirements for Smart Contracts based on Electronic Ledgers: ETSI DRAFT TR_119_540v0.0.6-public.pdf.

[15] This list is not exhaustive and national legislation is not included. The full references to the legislation are included at the end of this best practices report (link).

[16] https://www.europarl.europa.eu/factsheets/en/sheet/35/company-law.

7. Blockchain/DLT solutions for e-voting	Council of Europe's recommendation on standards for e-voting; Act concerning the election of the representatives of the Assembly by direct universal suffrage ; Council Decision (EU, Euratom) 2018/994; Compendium of E-voting and Other ICT Practices ; Council of Europe Recommendation CM/Rec (2017)5; Council of Europe CM (2022)10 Guidelines *[Not covered in the 1st cohort best practices report]*
8. Blockchain/DLT solutions enhancing CSRD compliance	Corporate Sustainability Reporting Directive (CSRD); European Sustainability Reporting Standards (ESRS) *[Not covered in the 1st cohort best practices report]*
10. Blockchain/DLT solutions enhancing compliance with the EUDR and the interplay with horizontal Data Regulation	Deforestation Regulation (EUDR) *[Not covered in the 1st cohort best practices report]*
9. Blockchain/DLT solutions for Battery Passports and DPPs and the interplay with horizontal Data Regulation	Battery Regulation / ESPR *[Chapter 7, 1st cohort best practices report]*
11. Compliance with the Data Governance Act and the Digital Services Act	Data Governance Act (DGA); Digital Services Act (DSA) *[Chapter 10, 1st cohort best practices report]*
12. Blockchain/DLT solutions to enhance compliance with sanctions lists	Sanctions lists *[Not covered in the 1st cohort best practices report]*
13. Blockchain/DLT solutions to enhance AML compliance	AMLD IV / AMLD V / TFR / DORA / AMLD V / AMLR *[Chapter 12, 1st cohort best practices report]*
14. DORA – Regulatory compliance	Digital Operational Resilience Act for the financial sector (DORA) *[DORA is not covered in the 1st cohort best practices report; NIS 2 is covered in Chapter 4 of the 1st cohort best practices report]*
15. Scope and delineation MiFID & MiCAR	MiFID II / MiFIR / AIFMD / CSDR / ECSPR / EMD II / PSD II / Prospectus Regulation / TFR / MiCAR / DLT-pilot Regime / TFR *[Chapters 13 and 14, 1st cohort best practices report]*
16. Use of the DLT Pilot Regime	Regulation on a pilot regime for market infrastructures based on distributed ledger technology (DLT Pilot Regime) *[Not specifically covered in the 1st cohort best practices report]*
17. Compliance with MiCAR	Regulation on markets in crypto-assets (MiCAR) *[Not specifically covered in the 1st cohort best practices report]*
18. Application of the ECSPR	European Crowdfunding Service Providers Regulation (ECSPR) *[Not specifically covered in the 1st cohort best practices report]*

19. Automated Markt Makers & Liquidity Pools	MiFID II, DLT Pilot Regime, MiCAR *[Not specifically covered in the 1st cohort best practices report]*

Some areas that were part of the regulatory dialogues in the 1st cohort were not covered in the 2nd round of dialogues, but may again become relevant for the 3rd round of dialogues such as Customs Regulation, prevention of trafficking in cultural assets and enhancing compliance with EU ETS/MRV reporting.

2.5. Looking ahead: the 3rd cohort

Many of the regulatory areas that were discussed in the 1st and the 2nd cohort will continue to be relevant for the 3rd cohort. Dialogues focused on these areas will allow for deeper dives into specific topics also in view new developments such as the publication of new secondary legislation, (draft) standards, new guidelines, administrative decisions and case law.

Moreover, the 3rd cohort of selected use cases includes a significant number of blockchain/DLT use cases that are based on a combination with other innovative technologies such as AI, IoT and Quantum Computing. Such combinations of innovative technologies are expected to trigger new elements for the regulatory dialogues including an increased emphasis on the AI Act and the intersection of the AI Act and other horizontal or industry specific regulation.

Finally the 3rd cohort will provide a basis for dialogues in relation to regulatory areas that could not be covered in the 1st and the 2nd cohort such as Blockchain/DLT solutions in the Health Care and the Energy sectors and the application of DAC7/8.

Areas for further clarification and dialogue for the 3rd cohort that have been identified during the 2nd round of dialogues are set out at the end of the sections 3 to 19 for each of the regulatory areas.

The ongoing developments in existing and proposed EU legislation and regulations and the required deeper dives into topics that were identified during the 1st and the 2nd round of dialogues underline the relevance of the fact that the European Blockchain Sandbox is set up as a longer term project.

3. Data Protection (GDPR) – Regulatory Compliance

3.1. Introduction

The GDPR was again one of the key regulatory areas for Blockchain/DLT solutions in the 2nd round of dialogues for the European Blockchain Sandbox.

Reference is made to Chapter 3 of the 1st cohort best practices report. In this section some parts of this report that served as a basis for the 2nd round of dialogues are quoted below in *blue*.

> *Report:*[17]
>
> - *A blockchain is a distributed but shared and synchronised digital database that is maintained by a consensus algorithm and stored on multiple nodes (computers that store a local version of the database). Blockchains can be imagined as a peer-to-peer network, with the nodes serving as the different peers. Some nodes only store a copy of the ledger whereas other nodes can also help process and validate transaction blocks as part of the consensus process so that they can be added to the permanent ledger of the blockchain. Data is collected, stored and processed in a decentralised manner in the form of blocks. Because these blocks are continuously added, but in principle never removed, a blockchain can be qualified as an append-only data structure.*
>
> - *The data that is recorded on the blockchain can relate to transactions (cryptographic digital signatures and timing of entries), digital content (documents, photos, videos, etc.) or applications (smart contracts). When this data directly or indirectly relates to an identified or identifiable natural person, it qualifies as personal data and data protection laws come into play.*
>
> - *In the EU, this means the Regulation (EU) 2016/6792016/679 or General Data Protection Regulation ("GDPR") applies. The GDPR provides for a harmonized set of rules for the processing of personal data by controllers and processors in the EU.*[18]
>
> - *As set out in Section 2 of the 1st cohort best practices report, different blockchain technologies have different characteristics. Compliance with the GDPR, depends to a large extent on the specific technical choices, and the governance set up of the use case. It is recommended to design the blockchain from the outset in a manner that takes the requirements of the GDPR into account, in accordance with the principles of data protection by design and default (Art. 25 GDPR).*

The 2nd round of dialogues provided a good basis to make deeper dives into some of the topics that were discussed in the 1st round and to discuss additional topics that were identified for discussion during this previous round of dialogues such as GDPR aspects of permissionless blockchains and the use of smart contracts in the context of Article 22 GDPR.

The lessons learned and best practices that were discussed during the 2nd round of dialogues are presented in the next paragraphs.

---

17 Quotation from chapter 3, 1st cohort best practices report (June 2024).

18 The EUI DPR (Regulation (EU) 2018/1725) provides for similar rules that are specifically aimed at the EU institutions, agencies and bodies that process personal data as controller or processor. The 1st round of dialogues focused on the GDPR.

3.2. Key question: Does the data recorded on the ledger qualify as personal data?

Report[19]:

- *Encrypting or hashing personal data is unlikely to make the data anonymous. In most cases, such data is only pseudonymized data which still qualifies as personal data.*
- *A case-by-case assessment is needed to determine if de-identification measures are sufficient to qualify data as anonymous data and therefore as non-personal data to which the GDPR requirements do not apply.*
- *ECJ case law and EDPB guidelines will be helpful to make this assessment, but important elements are still "work in progress".*
- *Data related to products are not personal data unless the data relates to an identifiable natural person (user/repairers or the use/handling by an identifiable natural person). If a data protection assessment has been made and it is shown that the data about products is only product-related without a link with an individual owner/user/repairer or that there is no risk of identification, then it can be assumed there is no personal data on the ledger.*
- *In the event of doubt, it is recommended to have an open discussion with the competent data protection authority before launching the service or to assume that data on the ledger could qualify as personal data and should be treated as such.*

The EDPB has published the draft guidelines regarding pseudonymization which were open for consultation responses until 28 February 2025.[20] In the consultation document it is confirmed that pseudonymized data, which could be attributed to a natural person by the use of additional information, remains information related to an identifiable natural person, and thus is personal data and that therefore the processing of such data needs to comply with the GDPR.

Several important developments are expected in the first half of 2025 including.

- The judgment in the CJEU SRB case summarized in the 1st cohort best practices report is expected in the 1st half year of 2025. The Conclusion of the Attorney-General became available on 6 February 2025 (Case C-413/23 P), available via this link).
- The EDPB guidelines regarding anonymization and blockchain are expected in the 1st half year of 2025.

The 3rd round of dialogues will provide the possibility to discuss the further clarifications and new insights that can be derived from these new developments

3.3. Application of the GDPR in the context of public permissionless blockchains

The use of public permissionless blockchains is allowed under GDPR, provided that the requirements of the GDPR are complied with.

Use case owners should assess the risks associated with the use of a certain technology and should take appropriate mitigating measures. Article 25 GDPR (*"Data protection by design and*

---

19 Quotation from chapter 3, 1st cohort best practices report (June 2024).

20 EDPB document 01/2025 of 16 January 2025. The consultation document can be accessed using this link: https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf.

by default") needs to be complied with but does not state anything about the need to use certain technologies. Companies need also to be able to demonstrate compliance with the rest of the obligations under the GDPR and especially in relation to data subject rights.

Generally speaking, important elements are to check what is stored on-chain, for what duration and how measures effect the historical data of transactions on the blockchain. Some specific observations regarding the application of the GDPR in connection with public permissionless blockchains that were discussed during the 2nd round of dialogues are set out below.

3.4. Data protection roles

Report[21]:

- *In a blockchain use case, different parties may separately process personal data in their systems. Such parties may be controllers if they determine purposes (why) and means (how) of the processing.[22] They may be processors if they only process personal data on behalf of other parties operating as controllers.[23]*

- *The GDPR assumes that the processor processes data on behalf of a controller governed by a contract or other legal act under Union or Member State law, and that there is a controller that can be identified for every element of the data processing route.[24] In accordance with the principle of accountability, it is necessary to assess the roles of all the parties using or involved in blockchain technologies. In this assessment, various elements need to be taken into account, such as, for instance, the nature of the service provided, the blockchain governance mechanism, the precise legal, technical and organisational characteristics of the blockchain, the relationships between the different actors involved, as well as the relevance of the processing of personal data within the scope of the service provided.*

Whenever there is processing of personal data there needs to be a controller that can take responsibility for compliance with the GDPR for every step in the process. In a decentralized setting there will normally be more parties involved in the processing of personal data and it is possible that different parties can take decisions or influence key elements of the processing of personal data either as separate or joint controllers in different steps in the process, such as authentication/identification of the user, recording of data on the ledger including the link to off-chain data and verification of data on the ledger.

For every step in the process the assessment needs to be made which party acts as (joint) controller and if (part of) the data processing is undertaken by one or more independent data processors.

Moreover, a processor in one step in the process could become a controller in another step. For instance, if a party qualifies as a data processor for the storage of a document in an off-chain location on behalf of the document's issuer (controller), this party could also qualify as an independent controller in the subsequent step in the process, for instance if such party then processes the document information no longer on behalf of the document's issuer to produce a hash (document ID) that is then recorded on-chain.

---

21 Quotation from chapter 3, 1st cohort best practices report (June 2024).
22 Art. 4(7); Art. 24 GDPR.
23 Art. 4(8); Art. 28 GDPR.
24 Art. 4(7) GDPR; https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en.

3.4.1. Qualification of the role of node operators in a public permissionless blockchain

The qualification of node operators in a **public permissionless blockchain** is challenging as node operators have limited control over the data that are recorded on the blockchain and use case owners are normally not able to give instructions about the processing of personal data and compliance with the GDPR to the node operators. Expected developments in 2025, including the judgment of the ECJ in the SRB case and the publication of the EDPB blockchain guidelines and the EDPB guidelines regarding anonymization which are expected in the first half of 2025 may provide more clarity.

However, it will probably need more time to resolve this issue unless blockchain specific legislation would be adopted.

3.4.2. The position of wallet providers

The provider of a self-hosted wallet would not per se qualify as a data controller or processor if the wallet is only running on the device of the end-user and there is no connection with an external platform. However, if the wallet is connected to an external platform then the wallet provider could qualify as controller even if no data is stored on this platform when the wallet provider determines purpose and means of the processing. A separate GDPR assessment is needed for each wallet.

With respect to the position of wallet providers, the outcome of the discussion regarding privacy risks and mitigations in relation to the EUDI Wallet could again helpful.[25] This would be a topic for further discussion in the context of the 3rd round of EBS dialogues.

3.4.3. Best practice regarding data protection roles

After the initial assessment of the roles of the parties involved and the identification of the controller(s), it is recommended to answer the following test questions for each step in the process:

- Are there any GDPR obligations that are not covered?
- Are there any GDPR obligations that other parties are better suited to address?

Depending on the answers the allocation of roles and/or the measures to ensure GDPR compliance may have to be adjusted.

3.5. Legal basis

Report[26]*:*

- "Performance of a contract" ("contractual necessity"), if applicable, can be an efficient legal basis for cross-border use cases, because the interpretation of this legal basis will generally not be dependent on national laws and interpretations (assuming that the contract contains a governing law provision).
- Other legal bases could also be relevant, depending on the characteristics of the use case:
  - "Legal obligation", if applicable, will depend on EU legislation or on the applicable EU or Member State national legislation.

[25] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/discussion-topics/a-privacy-risks-and-mitigations/.

[26] Quotation from chapter 3, 1st cohort best practices report (June 2024).

        - *Example: Battery passports / Digital Product Passports in relation to mandatory information.*
    - "Legitimate interest" would not be appropriate for the processing activities carried out by controllers that are public authorities in the performance of their tasks.
        - With respect to legitimate interest, it is important to apply the 3-step test set out in the EDPB Guidelines 1/2024 and supported by the CJEU case law (e.g., the cases C-13/16 (Rīgas satiksme), C-597/19 (M.I.C.M.), C-252/21 (Meta Platforms and Others) and C-621/22 (Koninklijke Nederlandse Lawn Tennisbond).[27]
        - *Possible example: Non-mandatory information in Digital Product Passports serving legitimate interests if the conditions are met.*
    - "Consent" from the data subject needs to meet strict requirements which can be problematic to comply with in practice:
        - *the consent must be freely given in order to be valid.*
        - *the data subject should be able to withdraw a given consent at any time and then the processing should be stopped which requires careful consideration in a blockchain context.*

- Please note that in order to rely on one of the above legal bases, the relevant conditions need to be met as set out in Art. 6 GDPR and further elaborated in case law and guidance.

Controllers are advised to carefully consider what is the most appropriate legal basis. In the event the data processing is regulated by a statutory regime, the most appropriate lawful basis to rely on in terms of the GDPR is likely Article 6(1)(c) of the GDPR (processing is necessary for compliance with a legal obligation to which the controller is subject) and the focus should be on what is necessary for compliance with the relevant legal obligation.

Example 1 – EU Company Certificate / Digital EU Power of Attorney:

- For mandatory personal data that needs to be included in the EU Company Certificate / Digital EU Power of Attorney on the basis of the national implementation of the Company Directive the legal basis will be "legal obligation".

- For non-mandatory personal data being collected by business registers on the basis of national law but for which inclusion in the EU Company Certificate is not mandatory in the national transposition of the proposed amendment of the Company Directive, the legal basis "task in the public interest" could be relevant.

- For a power of attorney that is not part of the EU Company Certificate or the Digital EU power of attorney and that is not published in the business register of the Member State the legal basis to consider could be "contractual obligation" if the data subject is a party to the contract with the Issuer as the data controller (which could be particularly relevant for the PoA – contract between the company and the authorized natural person).

Example 2 – AML/KYC legislation and the TFR:

- The processing of personal data under the AMLD/AMLR/TFR is subject to the GDPR with certain lex specialis provisions.[28]

---

[27] Firstly, the controller or the third party or parties to whom personal data are disclosed must pursue an interest that is legitimate (i.e., lawful). Secondly, to pursue the interest it must be necessary to process personal data. Thirdly, fundamental rights and freedoms of the data subjects must not take precedence over the interest pursued. The EDPB guidelines on the legal basis "legitimate interest" are available through this link.

[28] Transfer of Funds Regulation (TFR): Recitals (19), (34), (63); Article 25 (Data protection); Article 26 (Record retention). AMLD V: Chapter V – Data Protection, Record-retention and Statistical Data (Article 40 – Data

- In the context of AML/KYC legislation and the TFR the exception to the right to erasure in Article 17(3)(b) GDPR could be relevant in view of the specific legal obligations in relation to the processing of personal data in the AML/TFR and the national transpositions of the AMLD referenced in the previous paragraphs.[29]

The following approach could be helpful in order to be compliant with the GDPR (data protection by design/by default in line with Article 25 GDPR):

- First determine which data are mandatory and which data are optional.
- Splitting the use case up in two different GDPR processes: one for the mandatory data and one for the optional data.
- For the mandatory data "legal obligation" could be applied as a legal basis.
- For the optional data it is important to assess if there is another appropriate legal basis such as "contractual obligation".
- This distinction should be reflected in the documentation and in the workflow.

3.6. General data processing principles (focus on data minimisation, accuracy and transparency)

Article 5 GDPR lays down the general data processing principles that should be complied with, notably (a) 'lawfulness, fairness and transparency'; (b) 'purpose limitation'; (c) 'data minimisation'; (d) 'accuracy'; (e) 'storage limitation' and (f) 'integrity and confidentiality'. In accordance with Article 5(2) GDPR the controller shall be responsible for and be able to demonstrate compliance with these general data processing principles ('accountability').

If implemented correctly, blockchain can be a privacy enhancing technique, promoting compliance with the principles of minimisation, accuracy, integrity and confidentiality. The technology should be used in such a way as to ensure that personal data is retained in the on-chain space, and similarly in the pertinent off-chain location only to the extent that this is truly necessary for a proper operation of the use case and to ensure integrity and authenticity of verifications. Moreover, the fact that the data are stored in an encrypted/unintelligible form can be considered as furthering data minimisation.

Which measures need to be taken to ensure compliance with the data minimisation principle should be assessed by the data controller taking into account the specifics of the use case including the data flows, processes, data points, DLT operability and limitations including the controller's own general policies, and who is apt to determine whether the setup and data processing is ultimately in conformity with applicable data protection legislation.

Retention; Article 41 – Data Processing; Article 43 - The processing of personal data on the basis of this Directive for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 shall be considered to be a matter of public interest under Directive 95/46/EC). AMLD VI: Recitals (56), (122), (124); Article 70 - Processing of special categories of personal data referred to in Article 9(1) and personal data relating to criminal convictions and offences referred to in Article 10 GDPR by competent authorities; AMLR (Lex specialis provisions): Recitals (148), (150), (152), (157); Article 76 (Processing of personal data) - Processing of special categories of personal data referred to in Article 9(1) and personal data relating to criminal convictions and offences referred to in Article 10 GDPR by obliged entities; Article 77 - Record retention, including minimum 5-year data retention period in Article 77(3) AMLR and/or national AML laws; Article 78 - Provision of records to competent authorities.

[29] Art. 17(3)(*b) GDPR: for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*

In addition, it is crucial to exercise due care to ensure accurate data, through appropriate KYC processes if appropriate to verify that issuers that record data on the blockchain are the persons/organisations they purport to be.

Data accuracy is the responsibility for a data controller in every step of the process. Therefore, a data controller further down the process, who needs to rely on data that have been collected earlier by another party, still needs to comply with the data accuracy principle, including to accommodate data rectification requests; this may require appropriate contractual or other measures.

The transparency principle referred to in Article 5(1)(a) GDPR deserves specific attention in the DLT context. It is important to explain in an easily understandable way, despite technical complexities, how data is or may be processed.

Naturally, the controller should determine the optimum way in which to comply with the transparency principle, i.e. to convey its data processing operations and policy in clear and plain language, whilst faithfully reflecting the DLT ecosystem's scope. An option could perhaps be to include a diagram incorporated or annexed to the privacy statement for a better understanding which could be considered as a good practice going beyond the minimum requirements of the GDPR.

3.7. Data subject rights – right to erasure

Report[30]:

- *In principle the right to be forgotten / right to erasure could be implemented by breaking the link between the hash that is recorded on the ledger and the off-line storage, assuming a perfect cryptography/anonymization so that the hash cannot be reverse engineered to the personal data in the off-chain storage in any way. It should be noted that such an on-chain/off-chain architecture requires the use of another system in order to store the data itself. This means that there will also be a personal data processing in another component of the infrastructure which requires a separate risk assessment of this other system.*

Instead of "breaking the link" under the aforementioned conditions, complete deletion of the off-chain data might also be an option to comply with the right to erasure. In fact, such measures mean that the data recorded on-chain no longer qualify as personal data if, in the absence of the corresponding off-chain data, they cannot be attributed to an identifiable individual.

Additional arguments were shared in support of the findings regarding the right to erasure in the 1st cohort best practices report in favor of anonymization being equivalent with erasure. Indications that data erasure does not necessarily involve "complete destruction without leaving any trace" can be found in the Google Spain judgment of the CJEU, a decision from the Austrian DPA and the blockchain guidelines from the French DPA (CNIL).[31]

---

30 Quotation from chapter 3, 1st cohort best practices report (June 2024).

31 CJEU's judgement dated 13 May 2014 in the case C-131/12 ("Google Spain"), ECLI:EU:C:2014:317, available here (it states that having links to webpages removed from search results returned by a search engine operator stems from and satisfies the right to erasure); the Austrian DPA's decision dated 5 December 2018, DSB-D123.270/0009-DSB/2018, available here (it states that the data controller enjoys some flexibility in relation to the technical means which may be adopted, for realising erasure – and that anonymisation may be as one of these means); CNIL's blockchain guidelines, available here (the CNIL have acknowledged that erasure could possibly be obtained where the keyed hash function's secret key is deleted, along with the underlying personal data on other systems where it may have been stored for the purposes of processing).

Discussions about compliance with the GDPR by **public permissionless blockchains** including the right to erasure are ongoing and updated documents have been published since the 1st best practices report while further guidelines are expected. In chronological order:

- 13 November 2024 - The Spanish Data Protection Agency (AEPD) has published a technical note regarding Blockchain and the right to erasure and a video. The Proof of Concept presented in this document demonstrates the feasibility of building Blockchain infrastructures that allow compliance with the General Data Protection Regulation (GDPR) (The AEPD publishes a technical note in relation to Blockchain and the right to erasure | AEPD);

- 27 November 2024 – Publication of the report "Enhancing financial services with *permissionless blockchains", prepared for the European Commission (DG FISMA):*

  > *"The report examines the potential of public permissionless blockchains to enhance traditional financial services. It highlights the key advantages of utilising an open base layer, including transparency, inclusivity, and increased competition, while addressing critical challenges such as scalability, privacy, transaction sequencing, finality, and governance."*

- Publication of the EDPB Draft Guidelines on pseydonymisation (01/2025, available via: Guidelines 01/2025 on Pseudonymisation | European Data Protection Board).

- EDPB guidelines regarding anonymization and the EDPB blockchain guidelines are expected in the 1st half year of 2025.

- The expected judgment in the ECJ SRB-case. The Conclusion of the Attorney-General became available on 6 February 2025 (Case C-413/23 P), available via this link).

This area will likely – again - be an important topic for further discussion in the 3rd round of the EBS dialogues.

3.8. The use of smart contracts in the context of Article 22 GDPR

The application of smart contracts may trigger the applicability of Article 22 GDPR related to "automated individual decision-making, including profiling".

> *1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*
>
> *2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.*
>
> *3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.*
>
> *4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.*

It is important to assess if the processing of data through smart contracts does result in decisions which are binding for data subjects and produce legal effects for individual data subjects. If the smart contract only results in an option while human intervention is always needed for a binding decision, applicability of Article 22 GDPR will be less likely.

The smart contracts topic also requires further analysis for smart contracts for executing data sharing agreements in the sense of Article 36 Data Act: to what extent are the essential requirements laid down in Article 36 Data Act for such smart contracts relevant in the context of Article 22 GDPR? Further guidance is foreseen in Article 36 of the Data Act that is not yet available. Part of this further guidance might become relevant for the interpretation of the obligations on the basis of Article 22 GDPR.

3.9. GDPR compliance measures in the event of interoperability between DLT use cases

For the purposes of this document, interoperability between different blockchain networks is understood to be a two-way exchange of personal data between different blockchains.

- EU Blockchain Observatory and Forum, The current state of interoperability between blockchain networks, (c289f656-052a-4a72-b213-26b307691844_en (europa.eu):

  Par. 1.1: "Blockchain interoperability, referred to as 'the ability of *blockchain networks to communicate with each other, sending and receiving messages, data, and tokens' (Chainlink. (2023)) is therefore emerging as a requirement for the continuity of blockchain technology. Indeed, it will enhance productivity throughout the whole crypto sector because users can quickly move data and assets, which increases flexibility (Clarke, A. (2022))"*

From a data protection perspective such interoperability has implications for the data controllers and the data processors depending on if/to what extent each of them will be involved in the exchange and in what capacity. In order to the assess these implications and implement the necessary compliance measures the following checklist could be applied (to be discussed and adjusted/expanded in the next round of dialogues):

- Map which personal data will be shared
- Determine the parties' data protection roles (as controllers/processors)
- When sharing data with other controllers, e.g., external holder wallet providers:
  - Secure a legal basis for the sharing
  - Ensure the DP principles are met, e.g., the right quantity and quality of the data (data minimisation, accuracy)
- Put in place data processing agreements where certain processing activities are delegated to other parties, e.g., to nodes in other blockchains, other sub-processors
- Keep data secure when storing or transporting them to blockchain infrastructure controlled by other parties
- Amend the existing privacy notice to reflect changes to the data handling practices
- Map and safeguard any international transfers that might result from the exchange
- Ensure accountability

It would be advisable to keep interoperability in mind when designing the solution in particular if the use case is applied in areas where interoperability requirements could be applicable.[32]

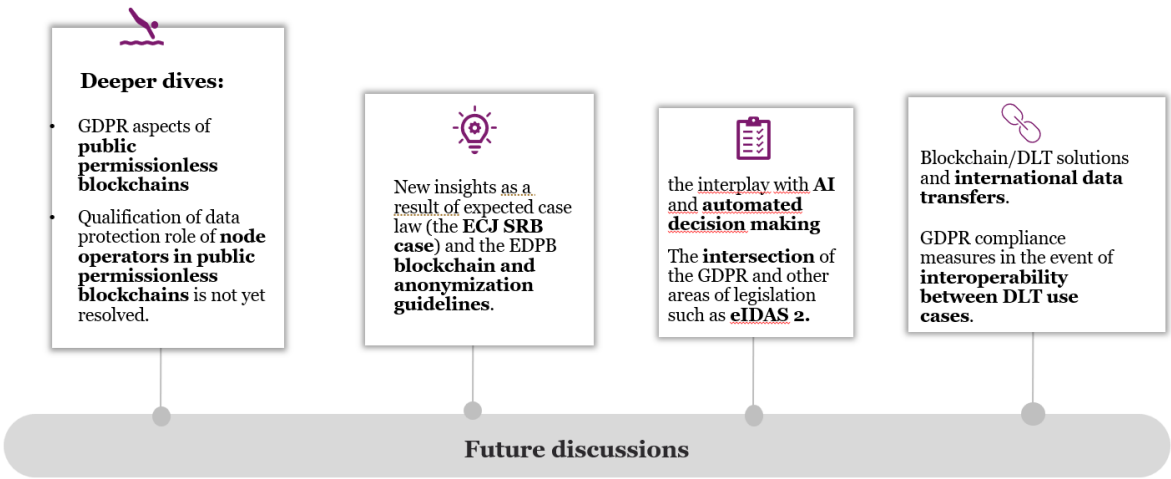
[32] See chapter 4 eIDAS; chapter 10 Battery Passports/DDP's and chapter 11 DGA/DSA.

3.10. The intersection of the GDPR and other areas of legislation

Compliance measures that need to be taken from a GDPR perspective need to be assessed in the context of other relevant regulation.[33] Other legislation may be relevant to determine which measures need to be taken and what data processing activities are or are not allowed. In some cases other regulation contains specific provisions that take precedence over the GDPR. In other cases regulation may provide a legal obligation as a legal basis in the sense of Article 6 GDPR. Examples of other relevant regulation are given in paragraph e) of this Chapter.

3.11. Topics for further discussion in the 3rd round of EBS dialogues

Several topics have been identified for discussion in more detail in the 3rd round of EBS dialogues, including new developments in case law and EDPB guidelines which are expected in the first half of 2025 and may also be relevant for GDPR aspects of public permissionless blockchains. Additional focus areas could be international data transfers and interoperability between DLT use cases as well as the interplay with other areas of regulation such as eIDAS 2[34] and the AI Act and automated decision making.



[33] See Article 23 GDPR.

[34] Reference is made to the discussion regarding privacy risks and mitigations in relation to the EUDI Wallet: A privacy risks and mitigations - EUDI Wallet

4. Relevance of the eIDAS regulation for Blockchain/DLT solutions

4.1. Introduction to the eIDAS chapter

This chapter will first discuss the relevance of the eIDAS regulatory framework for Blockchain/DLT solutions from a general perspective in paragraph a).

The eIDAS regulation was also one of the key regulatory areas for Blockchain/DLT solutions in the 1st round of dialogues for the European Blockchain Sandbox. Reference is made to Chapter 11 of the 1st cohort best practices report. In this section some parts of this report that served as a basis for the eIDAS focused 2nd round of dialogues are quoted below in blue.

The interplay between the eIDAS regulation and several other regulatory areas and applications is discussed in the next paragraphs:

- Interplay with the Company Directive (the EU company certificate and the Digital EU power of attorney) (Paragraph c)).
- Interplay with AML/KYC requirements in the AMLR (Paragraph d)).
- Interplay between the eIDAS regulation and Blockchain/DLT solutions in combination with IoT (Paragraph e)).

4.2. Relevance of the eIDAS regulatory framework for Blockchain/DLT solutions – General perspective

4.2.1. Introduction

Report:[35]

- *Regulation (EU) 2024/1183 of 11 April 2024 (**"eIDAS 2"**) amending Regulation (EU) No 910/2014 (**"eIDAS 1"**) has entered into force on 20 May 2024. eIDAS 2 covers the EUDI wallet, electronic identification schemes and trust services (both qualified and non-qualified). This is an important step towards harmonising digital identity and trust services across the EU.*

- *A notable change in eIDAS 2 is the introduction of the so-called **"European Digital Identity Wallet"** or **"EUDI Wallet"**. The first five implementing acts for the European Digital Identity Wallets have been published on 04 December 2024 in the EU Official Journal and entered into force on 24 December 2024.*

- *This new means of electronic identification allows users (natural persons and legal entities) to identify and authenticate themselves electronically, across borders, to access a wide range of public and private services. Additionally, users will be able to use it to sign documents with qualified electronic signatures (or electronic qualified seal) and as part of strong customer authentication (SCA) systems. The EUDI Wallet will also serve as the foundation for a common system to issue and validate attributes (qualified and unqualified) such as educational qualifications (including university degrees, other academic degrees and professional qualifications), driving licenses and permits.*

- *In addition, the list of **"trust services"** is significantly extended by eIDAS 2.*

[35] Chapter 11, 1st cohort best practices report (June 2024).

Article 3(16) eIDAS 1 as amended by eIDAS 2:
"trust service" means an electronic service normally provided for remuneration which consists of any of the following:
(a) the issuance of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services;
(b) the validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services;
(c) the creation of electronic signatures or electronic seals;
(d) the validation of electronic signatures or electronic seals;
(e) the preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals;
(f) the management of remote electronic signature creation devices or remote electronic seal creation devices;
(g) the issuance of electronic attestations of attributes;
(h) the validation of electronic attestation of attributes;
(i) the creation of electronic timestamps;
(j) the validation of electronic timestamps;
(k) the provision of electronic registered delivery services;
(l) the validation of data transmitted through electronic registered delivery services and related evidence;
(m) the electronic archiving of electronic data and electronic documents;
(n) the recording of electronic data in an electronic ledger".

- *New categories of trust services introduced by eIDAS 2 which can be particularly relevant for Blockchain/DLT applications include "electronic attestation of attributes", "electronic archiving services" and "electronic ledgers":*
    - *Management of remote qualified electronic signature creation devices and remote qualified electronic seal creation devices.*[36]
    - *'electronic attestation of attributes' means an attestation in electronic form that allows attributes to be authenticated.*[37]
    - *'electronic archiving' means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period.*[38]
    - *'electronic ledger' means a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records.*[39]

- *eIDAS 2 distinguishes between the requirements for non-qualified trust services and for qualified trust services which are both in scope of eIDAS 1. The regulatory requirements for both non-qualified and qualified trust services have become more stringent under the amended eIDAS 1 (see next paragraph).*

- *Qualified trust service providers have to be notified to the supervisory body together with a conformity assessment report.*[40] *In addition, qualified trust service providers must undergo an audit by a conformity assessment body at least every 24 months, at their*

[36] Art. 29a and Art. 39a eIDAS 2.
[37] Article 3(44) eIDAS Regulation as amended by eIDAS 2.
[38] Article 3(48) eIDAS Regulation as amended by eIDAS 2.
[39] Article 3(52) eIDAS Regulation as amended by eIDAS 2.
[40] Article 21 eIDAS Regulation as amended by eIDAS 2.

own expense.[41] *The conformity assessment report and the audit have to confirm that the providers and the qualified trust services they offer meet the requirements outlined in eIDAS 2.*[42]

- *eIDAS 2 is relevant for the provision of trust services not only in relation to qualified trust services but also in relation to non-qualified trust services. All trust services shall be made accessible for persons with disabilities and special needs as set out in Article 15 eIDAS 2 and should comply with the security requirements set out in Articles 19 and 19a of eIDAS 2. According to Article 19a(2) of eIDAS 2 the EC shall by 21 May 2025 establish a list of reference standards and where necessary establish specifications and procedures in relation to the provision of non-qualified trust services.*

- *An important difference between qualified and non-qualified trust services is the liability regime and the burden of proof which is much stricter for qualified trust service providers (Article 13 eIDAS 2). Another important difference is that the conformity assessment does not apply in relation to non-qualified trust services.*

- *eIDAS 2 refers to a range of implementing acts which need to be adopted by the European Commission, e.g. in relation to the EUDI Wallet, non-qualified trust services and qualified trust services.*

The EUDI Wallet will enable the user to securely request, obtain, select, combine, store, delete, share and present person identification data (**"PID"**)[43] and qualified and non-qualified Electronic Attestations of Attributes (**"EAAs"**)[44] to relying parties[45]. In addition, holders of an EUDI Wallet will be able to securely authenticate another persons' EUDI Wallet and to receive and share PIDs and EAAs in a secured way between the two EUDI Wallets.[46]

In view of the close relationship between qualified EAA services (**"QEAA"** services) and the EUDIW, the mandatory implementing acts pursuant to eIDAS 2 are intended to lay down similar requirements for the EUDI Wallet and QEAA services referring to European standards.[47]

On 3 June 2021, the European Commission adopted Recommendation (EU) 2021/946[48] on a Common Union Toolbox for a coordinated approach towards a European Digital Identity Framework calling on Member States to work closely together with the Commission towards the development of a Toolbox including a technical Architecture and Reference Framework (**"ARF"**), a set of common standards and technical specifications and a set of common guidelines and best practices. At the date of this document, release 1.8 of the ARF is available.[49]

---

41 Article 20 eIDAS Regulation as amended by eIDAS 2.

42 Article 20 and 21 eIDAS Regulation as amended by eIDAS 2. Following eIDAS 2 references to the cybersecurity risk management measures laid down in Article 21 of the NIS2 Directive have been added to Articles 20 and 21 of the eIDAS Regulation.

43 Commission Implementing Regulation (EU) 2024/2977 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets (Link).

44 Article 5a(4)(c) eIDAS 2 and the definitions of "attribute" (Art. 3(43) eIDAS2), "electronic attestation of attributes" in Art. 3(44) eIDAS 2 and "qualified electronic attestation of attributes" in Art. 3(45) eIDAS 2.

45 See definition of "relying party" in Art. 3(6) eIDAS 2.

46 EBSI-VECTOR – EBSI enabled Verifiable Credentials & Trusted Organisations Registries - Role of EBSI within eIDAS 2.0 of 1 June 2024: (Link).

47 Article 45d(5), Article 45e(2), Article 45f(6 & 7) eIDAS 2.

48 Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework.

49 https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.8.0/ .

4.2.2. Implementing Acts and the ARF

EIDAS 2 refers to a range of implementing acts which need to be adopted by the European Commission.

In particular, eIDAS 2 mandates implementing acts on the following issues:

- EUDI Wallet and Electronic Attestation of Attributes (by 21 November 2024).
- Reference standards and, where necessary, specifications and procedures for the requirements in relation to other trust services including electronic ledgers (by 21 May 2025).

The European Commission has adopted the following implementing acts thus far:

- Rules for the integrity and core functionalities of eID Wallets[50].
- Rules on the protocols and interfaces of eID Wallets solutions[51].
- Rules on person identification data and electronic attestations of attributes of eID Wallets[52].
- Reference standards, specifications and procedures for a certification framework for eID Wallets[53].
- Obligations for notifications to the Commission concerning the eID Wallet ecosystem[54].

The consultation phase for further implementing acts closed in early January and the final versions are expected soon during the first quarter of 2025.[55]

The eIDAS 2 Implementing Regulations determine the technology and standards applicable for the eIDAS 2 trust infrastructure. The Architecture and Reference Framework (**"ARF"**) based on Commission Recommendation (EU) 2021/946[56], defines how trust is established, maintained, validated, and managed among entities within the EUDI Wallet ecosystem. While the ARF is not legally binding, the eIDAS 2 Implementing Regulations regarding the EUDI Wallet specify that they must align with technology and standards developments and the work carried out under Recommendation (EU) 2021/946, particularly the ARF.

---

50 Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets

51 Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Framework.

52 Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets.

53 Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets.

54 Commission Implementing Regulation (EU) 2024/2980 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notifications to the Commission concerning the European Digital Identity Wallet ecosystem.

55 Link to (draft) implementing acts in various stages (Search for „910/2014") https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives_en?text=910/2014 with the consultation versions of the following implementing regulations: i) European Digital Identity Wallets – registration of relying parties, ii) European Digital Identity Wallets – security breaches, iii) European Digital Identity Wallets – list of certified wallets, iv) European digital identity framework – verification of electronic attestation of attributes and v) European Digital Identity Framework – cross-border identity matching.

56 Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework, and here.

Quotation report – Application of eIDAS 2 in relation to electronic ledgers

- *For qualified electronic ledgers the EC shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements specified in Article 45l of eIDAS 2 for qualified electronic ledgers: "(a) they are created and managed by one or more qualified trust service providers; (b) they establish the origin of data records in the ledger; (c) they ensure the unique sequential chronological ordering of data records in the ledger; (d) they record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time."*
- *How the use of DLT will be taken into account in applications for the grant of the "qualified status" for trust services will be regulated by means of implementing acts of the European Commission. A distinction will have to be made between:*
  - *Trust services **using** electronic ledger and*
  - *Trust services **providing** electronic ledger.*
- *"A trust service using ledger" can in theory also be qualified if the ledger that is used is not "qualified" as long as the requirements of eIDAS 2 are met but the ledger could be relevant to take into account as part of the conformity assessment of the "trust service using ledger". Clarity on how this will work out in practice in the implementing acts will be welcome.*

The (draft) Implementing Regulations on the basis of Article 45l (3) eIDAS 2 have not yet been published for consultation. The application of the provisions in the eIDAS 2 Regulation in relation to electronic ledgers will likely become a relevant topic for the next round of European Blockchain Sandbox dialogues.

4.2.3. Standards

The standards mentioned in the legally binding implementing acts determine the technology and standards applicable to the eIDAS trust infrastructure and have to be recognized by the Member States and the conformity assessment bodies.

- For the EUDI Wallet & trust services the standards mentioned in the implementing acts are the baseline, but Member States can apply additional national security standards (in line with the flexibility provided by the NIS2 Directive). This leads to additional work as regulators need to assess if the national standards are similar to the standards laid down in the implementing acts.
- For QEAA's and PUB_EAA's the baselines for the applicable standards will also be laid down in the implementing acts. There appears to be less room for additional national standards for QEAA's and PUB_EEA's (in line with the flexibility provided by the NIS2 Directive).
- For PUB_EAA's there is no need to go through a national conformity assessment on the basis of harmonized standards in the implementing acts. There will be a certification procedure for which the details are currently not yet clearly defined.

As mentioned eIDAS 2 is also relevant for the provision of non-qualified trust services. All trust services should comply with the security requirements set out in Articles 19 and 19a of eIDAS 2. According to Article 19a(2) of eIDAS 2 the EC shall by 21 May 2025 establish a list of reference standards and where necessary establish specifications and procedures in relation to the provision of non-qualified trust services.

4.2.3.1. General – eIDAS standards and standardization initiatives (not exhaustive)

The eIDAS framework includes several standards and standardisation initiatives aimed at ensuring interoperability and security across the EU which are not specifically focused for Blockchain/DLT.[57]

- ETSI:https://docbox.etsi.org/ESI/Open/workshops/202409_CEN_ETSI_Workshop/DAY1-1%20Overview%20of%20Standardization%20Plans/DAY1-1-35%20EUDIF%20Workshop%20Presentation%20-2024-09-10%20Nick%20Pope.pdf
- Trust Service Providers
- Architecture and reference framework - EUDI Wallet (Paragraph 9)

In particular, CEN (European Committee for Standardization), CENELEC (European Committee for Electrotechnical Standardization) and ETSI (European Telecommunications Standards Institute have already been developing eIDAS standardisation initiatives aimed at ensuring its interoperability and security across the EU.

4.2.3.2. eIDAS standards and standardization initiatives focused on blockchain/DLT (not exhaustive)

Regarding blockchain/DLT standards, the CEN-CENELEC working group 'Blockchain and Distributed Ledger Technologies' (CEN-CLC/JTC 19) was established based on the recommendations presented in the CEN-CENELEC White Paper on 'Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies'[58].

It identifies and adopts international standards already available or under development. The JTC works in close contact with ISO/TC 307 'Blockchain and distributed ledger technologies'. Furthermore, CEN-CLC/JTC 19 focuses on specific European legislative and policy requirements, in support of the development of the EU Digital Single Market.[59]

The report "Role of EBSI within eIDAS 2.0" refers in particular to the following standards relevant in the context of ledger and eIDAS:[60]

Committee	Standard	Scope	Status
ISO Tc 307	ISO 22739	Terminology	Final
	ISO TR 22349	Overview of existing DLT systems for identity management	Final
	ISO 23257	Reference Architecture	Final

[57] An overview of relevant eIDAS standards not specifically focused on blockchain and DLT's being developed by ETSI can be found here.

[58] See the following link: link.

[59] CEN-CLC/JTC 19 is currently working on the following standards as part of CEN/CLC JTC 19: "Activation PWI on Policy and Security Requirements on Trust Services on Electronic Ledger" (Emerging technologies - CEN-CENELEC), Environmental and sustainability classification methodology of consensus mechanisms of Blockchain and DLTs (prCEN/CLC/TR XXX (WI=JT019003)), Decentralised Identity Management Model based on Blockchain and other Distributed Ledgers Technologies. – Part 1: Generic Reference Framework (prCEN/CLC/TS XXXX (WI=JT019002)) and Blockchain and distributed ledger technologies - Vocabulary (ISO 22739:2024) (prEN ISO 22739 (WI=JT019004)).

[60] https://www.ebsi-vector.eu/wp-content/uploads/2025/02/Role-of-EBSI-within-eIDAS.pdf ; publication dates deliberately not included, as these are flexible.

	ISO TS 23635	Guidelines for governance	Final
	ISO TR 23644	Overview of trust anchors for DLT-based identity management	Final
	ISO DTR 24332 ISO TS 23353	Blockchain and DLT in relation to authoritative records, records systems, and records management Auditing Guidelines	Final draft Stabe draft
	ISO TS 23516	Interoperability Framework	Stable draft
CEN JTC 19	New Work Item	Policy and security requirements on QTSP for Ledger Basement: ISO TS 23353, ISO 23257, ISO 22739, ISO TS 23635 Compliance to: ETSI	Proposed

After completion of the eIDAS 2 focused dialogues for the 2nd round ETSI published the draft working document ETSI TR 119 540 V0.0.6 (2025-02) titled *"Electronic Signatures and Trust Infrastructures (ESI); Standardisation requirements for Smart Contracts based on Electronic Ledgers"*.[61] The draft document defines standardisation issues for Smart Contracts, as defined in the Data Act and based on Electronic Ledgers as defined by eIDAS 2 and can be discussed during the next round of dialogues.

4.2.3.3. Other eIDAS standards and standardization initiatives relevant for blockchain/DLT use cases (not exhaustive)

Other standards and standardization initiatives that are not specifically focused on Blockchain/DLT can also be particularly relevant such as in relation to trust services like electronic attestation of attributes, electronic archiving and electronic ledgers that can be particularly relevant for blockchain/DLT use cases.

Examples are the following draft standards regarding (Q)EAA's:

- Draft standard regarding Policy an Security requirements for Providers of Electronic Attestation of Attributes Services: ETSI DRAFT TS_119_471v0.0.11-public.pdf

[61] ETSI DRAFT TR_119_540v0.0.6-public.pdf

- Draft standard regarding (Q)EAA formats: https://docbox.etsi.org/esi/Open/Latest_Drafts/ETSI%20DRAFT%20TS_119_472-1v0.0.6-public.pdf

4.2.4. Best practices and lessons learned

4.2.4.1. Applicability of standards and harmonization

Blockchain/DLT use cases can benefit from the trust framework provided by the eIDAS regulation.

The ARF provides important guidance and may be critical for some use cases. Reference is made to the ARF Discussion Topics and Papers which provides a consultation forum: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/discussion-topics/.

The standards mentioned in the legally binding eIDAS Implementing Regulations determine the technology and standards applicable to the eIDAS trust infrastructure and have to be recognized by the Member States and the conformity assessment bodies. The eIDAS 2 Implementing Regulations regarding the EUDI Wallet specify that they must align with technology and standards developments in the context of the ARF.

The standards in the Implementing Regulations will be complemented by ETSI standards such as the standards for (Q)EAA profiles which are currently developed[62] and are expected to be published in Q3 2025. The implementing acts do not necessarily refer to these ETSI standards.

The question is if for instance the ETSI standards for EAA profiles[63] and the standards that are developed by CEN/CLC JTC 19 ("Activation PWI on Policy and Security Requirements on Trust Services on Electronic Ledger"[64]) can be applied by national conformity assessment bodies if/as long as these are not laid down in the implementing acts.

In order to enhance legal certainty, it would be welcome if the appropriate Blockchain/DLT standards are mentioned in the ARF and if the relevant standards become part of the regulatory framework through the necessary references in the eIDAS Implementing Regulations.

4.2.4.2. Use of blockchain/DLT solutions for trusted lists and registers of relying parties

Not only can Blockchain/DLT use cases benefit from the trust framework provided by the eIDAS regulation, the effective and efficient implementation of the eIDAS trust framework and the EUDI Wallet ecosystem can likely also benefit from blockchain/DLT solutions, for instance for the provisions of trusted lists and/or registers of relying parties.

- Each Member State is required to establish, maintain, and publish trusted lists (Article 22 eIDAS 2). The trusted lists must be electronically signed or sealed and published in a manner suitable for automated processing. This ensures the integrity and authenticity of the information, which is vital for Blockchain/DLT applications that rely on trust and transparency.

[62] https://docbox.etsi.org/esi/Open/Latest_Drafts/ETSI%20DRAFT%20TS_119_472-1v0.0.6-public.pdf.
[63] https://docbox.etsi.org/esi/Open/Latest_Drafts/ETSI%20DRAFT%20TS_119_472-1v0.0.6-public.pdf.
[64] CEN/CLC JTC 19 – "Activation PWI on Policy and Security Requirements on Trust Services on Electronic Ledger": Emerging technologies - CEN-CENELEC.

- Relying parties, which are entities that use the EUDI Wallet for providing services, must register in their respective Member States (Article 5b eIDAS 2). This registration process ensures that relying parties provide necessary information for authentication and intended use of the EUDI Wallet.

During the 2nd round of dialogues blockchain/DLT solutions were discussed that could be used for "trusted lists" or "registers of relying parties". See also the following publication from EBSI-VECTOR looking at the role of DLT for different parts of the eIDAS trust infrastructure (available via this link):[65]

> *"Beside the utilization of Electronic Ledger as infrastructure for EUDI Wallet or QTSP using Ledger the ledger can also be used as Trusted Registry meaning:*
>
> - *Issuer Registry*
> - *Verifier Registry.*
>
> *This would mean an Electronic Ledger could technically replace the existing TrustList acc. Art. 22 eIDAS resp. ETSI TS 119 612 which is currently implemented in XML. As with the new (qualified) trust services like QEAA the number of QTSP will foreseeably increase the current XML may not fulfill the required scalability across Europe."*

Topic X of the ARF concerns Relying Party Registrations as meant in Article 5b of eIDAS 2. The discussion on this topic X of the ARF on Relying Party Registration will start on the 12th of March 2025. This is a good time to present views about technology and standards requirements. See the following link: X - Relying Party registration · ARF Roadmap.

4.2.4.3. Identification of relevant electronic identification means and trust services

Quotation report - Relevance of eIDAS 2 for Blockchain/DLT solutions:

- *Pursuant to eIDAS 2 the list of "trust services" regulated by eIDAS 1 is extended. New categories of trust services which can be particularly relevant for Blockchain/DLT applications include "electronic attestation of attributes", "electronic archiving services" and "electronic ledgers".*
- *Blockchain/DLT solutions will normally qualify as trust services and/or will use trust services which are governed by eIDAS 2.*
- *eIDAS 2 is relevant for the provision of trust services not only in relation to qualified trust services but also in relation to non-qualified trust services.*
- *An important difference between qualified and non-qualified trust services is the liability regime and the burden of proof which is much stricter for qualified trust service providers (Article 13 eIDAS 2). Another important difference is that the conformity assessment does not apply in relation to non-qualified trust services.*

The use of blockchain/DLT solutions for electronic identification means or trust services are not precluded in eIDAS 2 or the Implementing Regulations as long as the regulatory requirements are met, and the relevant standards are complied with. For PID's the requirements will largely be determined on a national level. For (Q)EAA's blockchain/DLT solutions will normally have to make sure to have the DID of the issuer/holder as a reference in the (Q)EAA.

Depending on the use case a decision can be made which trust services (and with which level of assurance) would work best and if a combination with the EUDI Wallet and/or another electronic identification means is appropriate.

[65] Role of EBSI within eIDAS 2.0 page 21.

The mandatory PID information laid down in Implementing Regulation (EU) 2024/2977 is not always sufficient for identification in individual Member States.

- Regarding PIDs there is more room for national specifics by Member States.[66] Member States tend to require more information for natural and legal PID's than the mandatory information laid down in the Implementing Regulation 2024/2977. Other actors on a national level may also require more information depending on national or even sectoral law & regulations.

- An alternative for some use cases could be to use existing electronic identification means under eIDAS 1 for the time being

- Another option to explore in more detail (also in view of specific legal requirements for specific purposes such as AML/KYC compliance) is if PID information could be complemented by (Q)EAA's.[67]

QEAA's will be more harmonised than PID's and for non-qualified EAA's there is less regulation. There will be a consultation (relevant for both QEAA and non-QEAA). Reference is made to the following link:

https://docbox.etsi.org/esi/Open/Latest_Drafts/ETSI%20DRAFT%20TS_119_472-1v0.0.6-public.pdf).

Non-qualified trust services (including non-qualified EEA's) may also be considered as part of the mix. In relation to non-qualified trust services there is generally less regulation/harmonization[68] and the use of non-qualified trust services may as such not have the required level of assurance or legal effect. However, the combination with the EUDI Wallet and/or other (Q)TSPs could still be considered depending on the characteristics of the use case.

The following combined considerations (not exhaustive) might be of relevance:

- **Required level of assurance and trust:** How critical the data are and what is the necessary level of assurance or trust related to mutual recognition of the attributes or Digital Identity (PID)

  - Depending on the use case, the value of the protected information and the motivation of potential attackers could vary. This could lead to a variation in required levels of security (also at the edge).

  - Regulatory requirements in other relevant areas of regulation such as in relation to AML, ESG reporting and the EU Corporate Certificate may require a certain minimum level of assurance or trust.[69]

- **Differences in legal consequences** between non-qualified and qualified trust services effect of qualified trust services:

  - Desired legal effect: the legal effect of a qualified electronic signature is comparable with a handwritten signature and a QEAA has the same legal effect as a lawfully issued

66 See ARF paragraph 3.4.
67 See ARF paragraphs 5.2, 5.3 and 5.4. Although a PID is a necessary part to set a EUID Wallet to the status 'Valid', and (Q)EAA's cannot be a formal part thereof, the PID could possibly, and depending on the use case, be complemented by (Q)EAA's.
68 Although eIDAS 2 provides a framework for non-qualified trust services and cyber security legislation will be applicable. See chapter 11 of the 1st best practices report.
69 Reference is made to paragraph 4.3, 4.4, 8 and 13 of this best practices report.

attestation in paper form. eIDAS2 contains similar provisions in relation to legal effect for other qualified trust services.[70]

- Another important difference between qualified and non-qualified trust services is the liability regime and the burden of proof which is much stricter for qualified trust service providers (Article 13 eIDAS 2). Moreover, the conformity assessment does not apply in relation to non-qualified trust services.

- **"Make or buy":** What is already available on the market and is it preferred to develop a solution with own resources or to make use (in total or in part) of solutions which were already foreseen in eIDAS1 such as advanced or qualified electronic signatures, qualified time stamps or advanced or qualified electronic seals.

- **Timing:** eIDAS1 such as electronic identification schemes, advanced/qualified signatures, qualified time stamps and advanced/qualified electronic seals and also attestations of attributes are available and can be issued in any system or wallet, while the EUDI Wallet will become available by the end of 2026 and the Implementing Acts and standards on the basis of eIDAS 2 in connection with other trust services that are introduced by eIDAS 2 are still being developed.

- **Interoperability:** the possibility to migrate from eIDAS1 trust services/electronic identification to trust services and electronic identification such as the EUDI Wallet that will become available in the future.

4.2.5. Areas for further dialogue and clarification

Several topics have been identified for discussion in more detail in the 3rd round of EBS dialogues:

- The new/additional Implementing Acts and standards that are currently being developed on the basis of eIDAS 2 will provide new insights. In particular the (draft) Implementing Regulations on the basis of Article 45l(3) eIDAS 2 regarding electronic ledgers and the development of standardization requirements for smart contracts based on electronic ledgers will be relevant for DLT use cases.

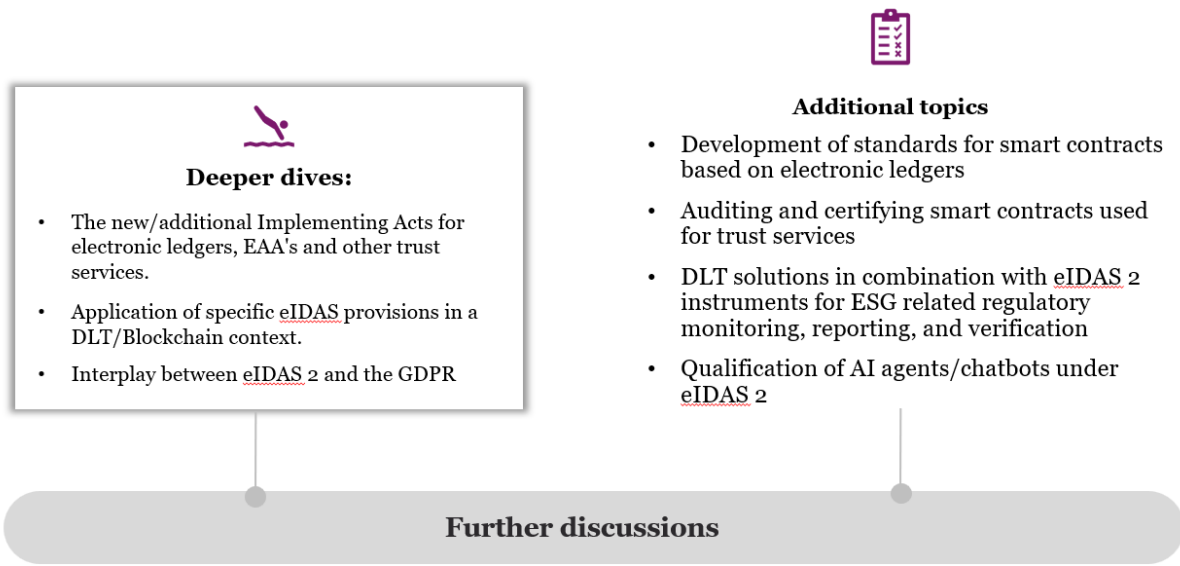
- Deeper dives into specific topics such as using DLT for (1) Selective Disclosure i.r.t. article 5a, point 4a of the eIDAS revision (2024/1183), (2) the access rights of Relying Parties (implementing acts as regards the registration of wallet-relying parties) and (3) logging transactions carried out through the EU DIW i.r.t. article 5a, point 4d.

- Auditing and certification of smart contracts in the context of the development and deployment of trust services.

- The use of DLT solutions (in combination with other innovative technologies such as AI and/or IoT) in combination with eIDAS 2 regulatory instruments for compliance with (regulatory) monitoring, reporting and verification obligations.

- The interplay between the eIDAS regulation and the GDPR is one of the topics for further discussion as part of the 3rd round of EBS dialogues. Reference is made to the discussion regarding privacy risks and mitigations in relation to the EUDI Wallet: A privacy risks and mitigations - EUDI Wallet.

[70] See Art. 25(2) eIDAS for qualified electronic signatures and Art. 45b(2) eIDAS 2 for QEAA services. Other provisions in eIDAS 2 relating to the legal effect of other qualified trust services include Art. 24a (Recognition of qualified trust services), Art. 35(2) (electronic seals), Art. 41(2) (electronic time stamps), 43(2) (electronic registered delivery services), 45(1a) (website authentication), 45i(2) (electronic archiving), 45k(2) (electronic ledgers).



4.3. Interplay between eIDAS & Company Directive – EU company certificate and Digital EU power of attorney

4.3.1. Introduction

The Company Directive[71] lays down minimum requirements for the publication of information in relation to limited liability companies by the business registers of the Member States.[72] The registration obligations have been extended to certain partnerships in a further amendment of the Company Directive by Directive (EU) 2025/25.[73] The provisions of Directive 2025/25 will need to be transposed in national legislation by **31 July 2027** and the national provisions should become applicable from **31 July 2028**.[74]

According to Article 16b of the amended Company Directive the Member States will have to ensure that their business registers issue EU Company Certificates for the limited liability companies and partnerships that are in scope of the Company Directive. According to Article 16b (1) of the amended Company Directive, the EU Company Certificate shall be accepted in all Member States as sufficient evidence, at the time of its issuance, of the incorporation of the company and of the information listed in Article 16b(2) & (3) of the Company Directive for limited liability companies and certain partnerships.

The EU Company Certificate for limited liability companies and partnerships in scope of the Company Directive shall include the following information:

Limited liability companies (Article 16b (2))	Partnerships (Article 16b (3))
(a) the name or names of the company;	Same
(b) the legal form of the company;	Same

71 Directive (EU) 2017/1132, most recently amended by Directive 2025/25.
72 Articles 14 – 16 Company Directive (EU) 2017/1132 as most recently amended by Directive 2025/25 of 19 December 2024 (LINK).
73 Article 14a Company Directive (EU) 2017/1132 as most recently amended by Directive 2025/25 of 19 December 2024 (LINK).
74 Article 4(1) & (2) Directive 2025/25.

Limited liability companies (Article 16b (2))	Partnerships (Article 16b (3))
(c) the registration number of the company and the Member State where the company is registered;	Same
(d) the EUID of the company;	Same
(e) the registered office of the company;	(a) the registered office, or equivalent, of the partnership;
(f) the correspondence address of the company, such as its electronic mail or postal address;	Same
(g) the date of registration of the company;	Same
(h) the amount of the subscribed capital of the company, if applicable;	(b) the amount of maximum liability or of the contribution of each limited partner, where that information is recorded in the national register;
(i) the status of the company, such as when it is closed, struck off the register, wound up, dissolved, undergoing insolvency proceedings, economically active or inactive as defined in national law and where it is recorded in the national register;	Same
(j) the first names, surnames and date of birth, or equivalent information when that date is not recorded in the national register, of any persons who either as a body or as members of any such body are authorised by the company to represent it in dealings with third parties and in legal proceedings, and whether those persons may do so alone or are required to act jointly;	(c) the first names, surnames and date of birth, or equivalent information when that date is not recorded in the national register, of the partners, directors or other statutory representatives, who are authorised to represent the partnership in dealings with third parties and in legal proceedings, or, if not applicable, information about the nature and scope of the authorisation of the partners, directors or other representatives to represent the partnership and their particulars;
(k) where the persons referred to in point (j) are legal persons, the name, the legal form, the EUID or, where the EUID is not applicable, the registration number;	(d) where the persons referred to in point (c) are legal persons, the name, the legal form, the EUID or, where the EUID is not applicable, the registration number; (
	e) where different from points (c) and (d), the first names, surnames and date of birth, or equivalent information when that date is not recorded in the national register, of the general partners, and, in the case of limited partnerships, particulars of the limited partners, where particulars of the latter are made publicly available in the national register;
	(f) where the persons referred to in point (e) are legal persons, the name, the legal form, the EUID or, where the EUID is not applicable, the registration number
(l) the object of the company, describing its main activity or activities, which can be expressed using the relevant Statistical Classification of Economic Activities in the European Community (NACE) code, where such code is used for the purposes of the register pursuant to applicable national law, and where the object is recorded in the national register;	Same
(m) the duration of the company, where its duration is limited;	Same

Limited liability companies (Article 16b (2))	Partnerships (Article 16b (3))
(n) details of the company's website where such details are recorded in the national register;	Same
(o) the date of issue of the company's EU Company Certificate.	Same

The information that is made available through the EU Company Certificate for limited liability companies and certain partnerships is partly more extensive and partly different from the LPID information that will be part of the EUDI Wallet on the basis of the current version of the relevant eIDAS Implementing Regulation.[75]

The Company Directive requires that the EU Company Certificate can be obtained from the business registers upon an application in electronic or paper form (or through the system of interconnection of registers).[76] The EU Company Certificate in electronic format should be free of charge unless it causes serious prejudice to the financing of the business registers in which case the price shall not exceed the costs. In any event each company shall be able to obtain its Company Certificate free of charge at least once per calendar year.[77]

According to Article 16b(6) of the Company Directive, Member States shall ensure that the EU Company Certificate is authenticated by means of **trust services** as referred to in the eIDAS regulation. The EU Company Certificate shall also be compatible with the **European Digital Identity Wallet**.

According to Article 24(2)(d) of the Company Directive the Commission shall adopt:

(d) the technical specifications including the compatibility with the European Digital Identity Wallet as provided for in Regulation (EU) 2024/1183, as well as the taxonomy and the multilingual template for the EU Company Certificate referred to in Article 16b of this Directive;

4.3.2. Electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source

Article 45f eIDAS 2 lays down requirements for electronic attestation of attributes issued by or on behalf of a public sector boy responsible for an authentic source.

- 3(7) **'public sector body'** means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;

---

75 Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 regarding person identification data and electronic attestations of attributes issued to European Digital Identity Wallets. The Annex specifies the mandatory and optional LPID information which is limited to the current legal name and a unique identifier in the Member State and optioally the current address and additional registration numbers (VAT, tax, EUI, LEI, EORI and the number following Council Regulation (EU) No 389/2012).

76 Article 16b(4) of the amended Company Directive.

77 According to Article 16c of the amended Company Directive the Member States shall also ensure that in order to carry out *certain procedures in scope of the Directive*, companies in scope of the directive can use a template for a digital EU power of attorney to authorize a person to represent the company. The scope of the digital EU power of attorney is, however, limited to the authority to carry out certain procedures in scope of the Directive such as the formation of companies, the registration or closure of branches and cross-border conversions, mergers and divisions.

- 3(46) **'electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source'** means an electronic attestation of attributes issued by a public sector body that is responsible for an authentic source or by a public sector body that is designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45f and with Annex VII;

- 3(47) **'authentic source'** means a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice;

The business registers in the Member States qualify as "public sector body" holding an "authentic source" in relation to the issuing an EU Company Certificate. The EU Company Certificate itself will qualify as "electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source" (**"PUB_EEA"**).

As mentioned above, the use of the EU Company Certificate by qualified trust service providers is facilitated through article 16b point 6 of the amendment (2025/25) of the Company Directive, stating that the EU Company Certificate should be authenticated by means of trust services and that should be compatible with the EU Digital Identity Wallet. Article 16b point 6 is partially "complemented" by Article 45e eIDAS 2 Regulation which requires Member States to ensure that - by the end of December 2026[78], at least for the minimum list of attributes listed in Annex VI to the eIDAS 2 Regulation, wherever those attributes rely on authentic sources within the pubic sector - measures are taken to allow qualified trust service providers of EAAs to verify those attributes by electronic means at the request of the user. The EU Company Certificate partially overlaps with two required categories of minimum data (annex VI): "powers and mandates..." and "financial and company data".

4.3.3. Best practices and lessons learned

The use of blockchain/DLT solutions for the issuance of EU Company Certificates is not precluded in the amended Company Directive and can be an option to consider (whether or not together with a centralized solution) by the business registers in the Member States when implementing the EU Company Certificate provisions.

The mandatory and optional LPID information categories specified in the Annex to Commission Implementing Regulation 2024/2977 appears not sufficient for commercial business. For commercial business the LPID will likely need to be combined with the EU Company Certificate and a power of attorney.

Most of the LPID data on the basis of eIDAS 2 Implementing Regulation 2024/2977 appear to be included in the EU Company Certificate, meaning that the question comes up if the LPID and the EU Company Certificate could become one and the same for the companies (limited liability companies and partnerships) that are in scope of the Company Directive.

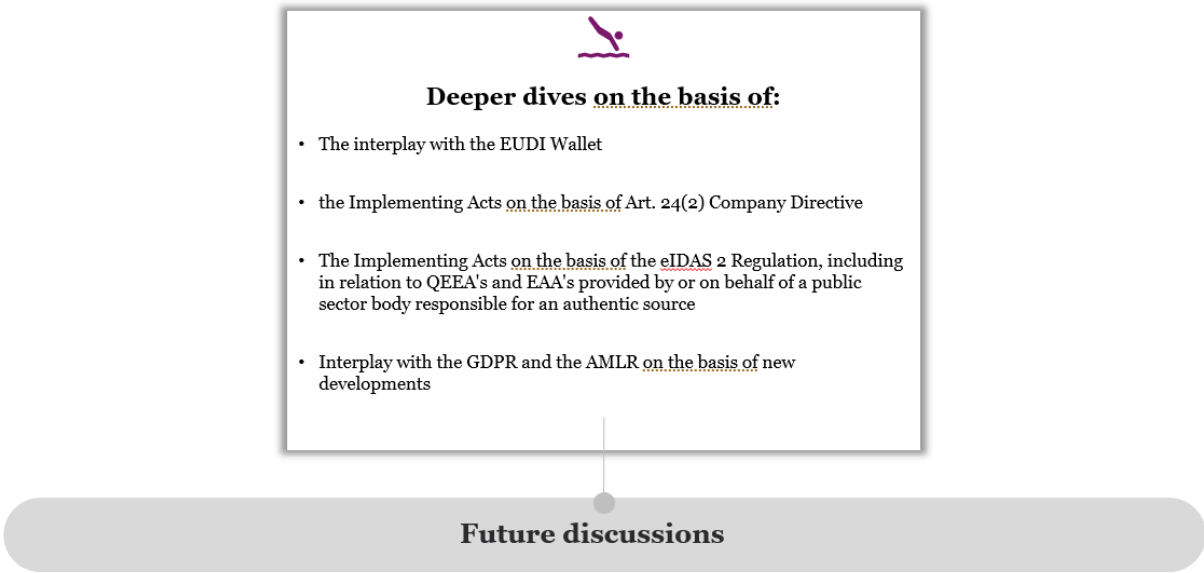
However, in practice, a combination of instruments will still be needed. While the EU Company Certificate does include information about the company and the mandate of a natural person authorized to represent this company, proof will still be needed that the person who presents this information is the person referred to in the EU Company Certificate. An interplay between the (Q)EAA's of the natural person acting on behalf of, and the (Q)EAA's of the legal entity are needed to establish the relation between those two. The combination of instruments can be facilitated further as part of the technical specifications to be adopted by the European

[78] Within 24 months of the date of entry into force of the implementing acts referred to in Article 5a(23) and 5c(6) which were published on 4 December 2024.

Commission on the basis of Article 24(2)(d) to ensure the compatibility of the EU Company Certificate with the EUDI Wallet and the template for the EU Company Certificate that will be published by the Commission on the basis of Article 16b(8) of the Company Directive.

Regardless of the information that is included in the EU Company Certificate, information that is published in the business registers in accordance with the national laws implementing the Company Directive, including with respect to authorized representatives of the companies in scope of the amended Company Directive[79], appears to qualify as PUB_EAAs in the sense of Article 45f eIDAS 2. If this is the correct interpretation, such information can be verified by QTSPs against the information in the business register in the sense of Article 45e eIDAS once this provision becomes applicable (by the end of 2026). However, there may still be room for Member States to (partially) implement these provisions in another way – depending on the respective tasks, data availability and technical capabilities of the business registers.

Information about authorized representatives not registered in the business registers does not qualify as PUB_EAA. Such information about company representatives qualifies as EAAs or QEAAs depending on whether the attributes are provided by a TSP or QTSP.



[79] And therefore, not limited in scope to certain procedures relevant for the digital EU power of attorney in Article 16c of the amended Company Directive.

4.4. Interplay between eIDAS & AML/KYC Requirements in the AMLR

4.4.1. Introduction

Article 3 of the AMLR specifies the obliged entities that need to comply with the AML/KYC requirements laid down in the AMLR. The Customer due diligence measures that need to be applied by the obliged entities are laid down in Article 20 AMLR. Most of measures referred to in Article 20 AMLR can be applied by using data from authentic sources or QEAA's.

Potential EAA's for AML/KYC compliance

Customer due diligence measures (Article 20 AMLR)	Examples of trusted sources
(a) identifying the customer and verifying the customer's identity;	EUDI Wallet, other electronic identification means
(b) identifying the beneficial owners and taking reasonable measures to verify their identity so that the obliged entity is satisfied that it knows who the beneficial owner is and that it understands the ownership and control structure of the customer;	UBO Register information (Authentic Source) Notaries? (Authentic source?) QTSP using authentic sources
(c) assessing and, as appropriate, obtaining information on and understanding the purpose and intended nature of the business relationship or the occasional transactions;	Specific. QTSP for certain relevant attributes such as tax history or bank account number
(d) verifying whether the customer or the beneficial owners are subject to targeted financial sanctions, and, in the case of a customer or party to a legal arrangement who is a legal entity, whether natural or legal persons subject to targeted financial sanctions control the legal entity or have more than 50 % of the proprietary rights of that legal entity or majority interest in it, whether individually or collectively;	Sanctions registers (Authentic source?) QTSP
(e) assessing and, as appropriate, obtaining information on the nature of the customers' business, including, in the case of undertakings, whether they carry out activities, or of their employment or occupation;	Commercial registers (Authentic source) QTSP using authentic sources
(f) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds;	Specific
(g) determining whether the customer, the beneficial owner of the customer and, where relevant, the person on whose behalf or for the benefit of whom a transaction or activity is being carried out is a politically exposed person, a family member or person known to be a close associate;	PEP register (authentic source) QTSP using authentic source
(h) where a transaction or activity is being conducted on behalf of or for the benefit of natural persons other than the customer, identifying and verifying the identity of those natural persons;	EUDI Wallet, other electronic identification means
(i) verifying that any person purporting to act on behalf of the customer is so authorized and identify and verify their identity.	Notaries? (Authentic source) QTSP EUDI Wallet, other electronic identification means

The AMLR provides[80] that obliged entities must obtain the necessary information, documents, and data to verify the identity of customers and any persons acting on their behalf through the following means:

(a) the submission of an identity document, passport or equivalent and, where relevant, the acquisition of information from reliable and independent sources, whether accessed directly or provided by the customer;

(b) the use of electronic identification means which meet the requirements of Regulation (EU) No 910/2014 with regard to the assurance levels 'substantial' or 'high' and relevant qualified trust services as set out in that Regulation.

By 10 July 2026[81], the Anti-Money Laundering Authority (AMLA) will a.o. develop draft regulatory technical standards specifying the list of attributes that electronic identification means and relevant qualified trust services must feature to fulfill the requirements for standard, simplified, and enhanced due diligence.

The AMLR provides room for obliged entities to rely on measures taken by other obliged entities for compliance with the AML/KYC requirements under certain conditions.[82] Article 49 AMLR states that obliged entities shall obtain from the obliged entity relied upon all the

80 Article 22(6) AMLR.
81 Article 28 AMLR.
82 Article 48 AMLR

necessary information concerning the customer due diligence measures laid down in Article 20(1), points (a), (b) and (c), or the business being introduced.

Obliged entities which rely on other obliged entities shall take all necessary steps to ensure that the obliged entity relied upon provides, upon request:

(a) copies of the information collected to identify the customer;

(b) all supporting documents or trustworthy sources of information that were used to verify the identity of the client, and, where relevant, of the customer's beneficial owners or persons on whose behalf the customer acts, including data obtained through electronic identification means and relevant trust services as set out in Regulation (EU) No 910/2014; and

(c) any information collected on the purpose and intended nature of the business relationship.

4.4.2. Best practices and lessons learned

Several use cases have been discussed during the 2nd round of dialogues using blockchain as a suitable means for decentralized, secure and privacy preserving exchange of information or verifying identities.

Currently AML requirements vary across Member States, but the AML regulatory framework will become more harmonized under AMLR/AMLD VI.

The mandatory PID information in Implementing Regulation (EU) 2024/2977 is not always sufficient for identification, necessitating additional attributes as per national legislation. It means that obliged entities are obliged to collect other attributes to complement the data in accordance with national legislation.

However, the EUDI Wallet ecosystem in combination with (Q)EAA's and Pub_EAA's creates a new way to collect necessary verifiable data directly from the user. Such an approach is sometimes identified as a "Reusable KYC". The interplay between privacy and the gatekeepers' obligations under AML is relevant. Strong privacy preserving networks/solutions are needed on EU level.

The EUDI Wallet ecosystem usage in combination with the trust infrastructure in compliance with the eIDAS regulation creates new possibilities to digitalize and consequently simplify AML compliance processes and increase data quality.

As long as the EUDI Wallet is not implemented, it may be relevant to consider electronic identification means under eIDAS 1, as there are already schemes and providers offering assurance levels 'substantial' or 'high' that are accepted and can be used across the EU. For instance, the Belgian ITSME system can be used in the Netherlands with a high level of assurance.

An "advanced e-signature" is not always sufficient for the assurance level "substantial" referred to in Article 22(6) AMLR. There will likely be an implementing act on the basis of Article 26 eIDAS 2 to set minimum requirements for advanced e-signatures.

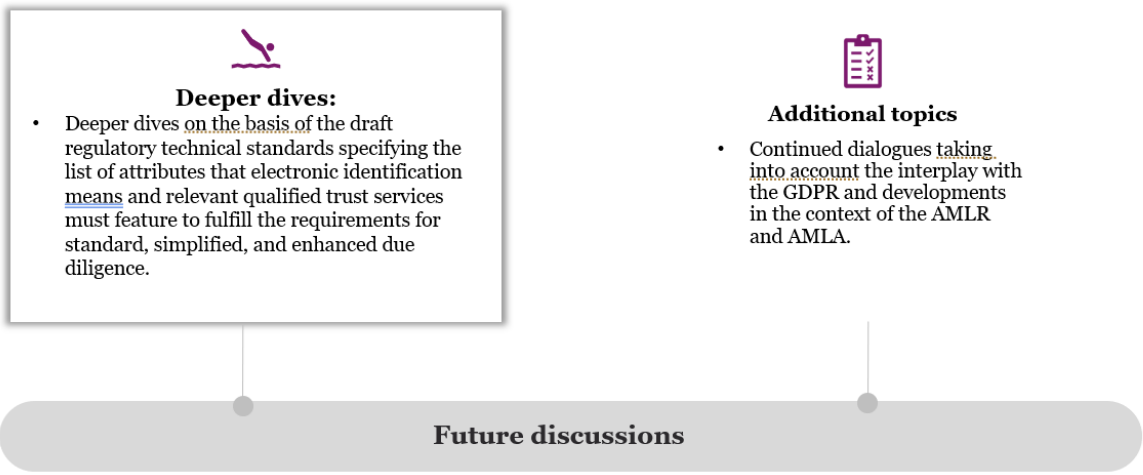
Currently information for AML/KYC checks is proven on paper which is relatively easy to forge. Blockchain/DLT use cases that make use of trustworthy eIDAS regulatory tools that meet the criteria of the AMLR:

- can help ensure that data is not tampered with, through electronic mean: where the data is coming from and the status of the data.

- can be an opportunity to standardize/automate filing processes for certain occupations, such as notaries, lawyers or tax advisors that are currently performing these tasks (most 0ften) manually.
- can facilitate the re-use of certain trustworthy information concerning the customer due diligence measures.
- can facilitate audits by competent authorities.

4.4.3. Areas for further dialogue and clarification

Further developments are expected for instance the development of draft regulatory technical standards specifying the list of attributes that electronic identification means and relevant qualified trust services must feature to fulfill the requirements for standard, simplified, and enhanced due diligence and other developments in the context of the AMLR and AMLA.



4.5. Interplay between eIDAS & IoT devices

4.5.1. Wallets for objects such as IoT devices?

The EUDI Wallet can only be used by natural persons and legal entities. Machine-to-machine and IoT hardware require identifier wallets for "objects", not identity wallets such as the EUDI Wallet. Everything except for PID (person identification data) can qualify as attributes and attributes do not necessarily need to be machine-readable. Identifiers for objects mean identifiers for processes, hardware and software which can qualify as attributes in the sense of the eIDAS 2 regulation.

An important question is whether the attributes for IoT devices are 'wrappable' in a machine wallet (not an EUDIW/personal wallet) that comprises the attributes. Another question is if the (wrapped) attributes that are verifiable through the ledger can serve as a trustworthy "oracle"[83] which can qualify as QEAAs that meet the requirements of the eIDAS 2 regulatory framework.

There are at the moment no recommendations or advice regarding wallets for machines and IoT devices. It might be helpful if a standard for these machine/device wallets would be developed.

[83] Definition by the ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLR): *"6.21 DLT oracle: service that supplies information to a distributed ledger using data from outside of a distributed ledger system."* Distributed ledger technology terms and definitions.

Depending on the use case, different (combinations of) trust services and possibly electronic identification means could be considered (see next paragraph).

4.5.2. Relevant eIDAS 2 regulatory instruments for DLT/IoT solutions

Wallets for legal and natural persons (for example the EUDI Wallet) can be used by the holders of such wallets to present a statement about the facts in connection with a certain object.

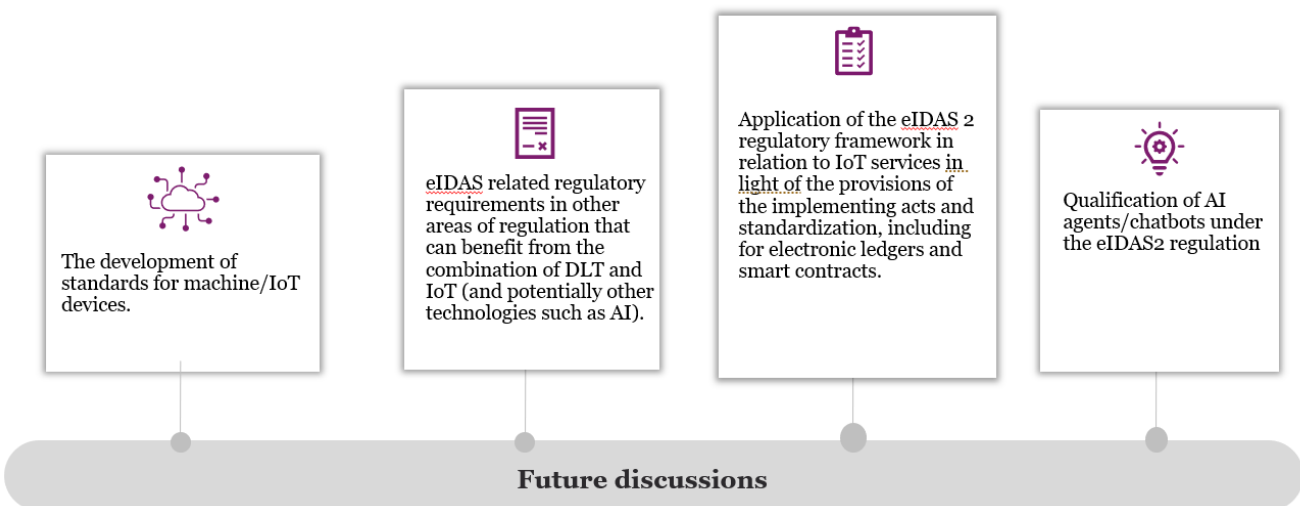
However, trust service providers do not necessarily need to use a wallet for the presentation of attributes related to IoT devices. Another option might be to use a combination of (Q)EEA's whether or not in combination with eIDAS 1 trust services such as an electronic seal (simple, advanced or qualified) or an electronic time stamp (simple or qualified) and an electronic signature (simple, advanced or qualified).

Depending on the use case a decision can be made which trust services (and with which level of assurance) would work best and if a combination with the EUDI Wallet or another electronic identification means is appropriate.[84]

4.5.3. Areas for further discussion:

The following areas for further clarification and future regulatory dialogues have been identified:

- The development of standards for machine/IoT devices.
- eIDAS related regulatory requirements in other areas of regulation that can benefit from the combination of DLT and IoT (and potentially other technologies such as AI).
- Application of the eIDAS 2 regulatory framework in relation to IoT services in light of the provisions of the implementing acts and standardization, including for electronic ledgers and smart contracts.
- Qualification of AI agents/chatbots under the eIDAS2 regulation



[84] See paragraph 4.2.4.

5. Blockchain/DLT and AI

5.1. Introduction

The Artificial Intelligence Act (Regulation (EU) 2024/1689 of 13 June 2024) was published in June of 2024. The AI Act lays down harmonised rules on artificial intelligence. Its goal is to mainly provide AI developers and deployers with clear requirements and obligations regarding specific uses of AI, with a particular focus on high-risk AI systems and general-purpose AI models that pose systemic risks which should apply also when these models are integrated or form part of an AI system. At the same time, the regulation seeks to reduce administrative and financial burdens for business, in particular small and medium-sized enterprises.

Article 3(1) and 3(63) AI Act defines "AI system" and "general purpose AI model":

- Art. 3(1) ***'AI system'*** *means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;*

- Art. 3(63) ***'general-purpose AI model'*** *means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market;*

Furthermore, a distinction is made between 'providers' and 'third-party (suppliers)' under the AI Act in the definitions and the recitals:

- Art. (3) ***'provider'*** *means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge;*

- Article 25(1) AI Act - *Any distributor, importer, deployer* ***or other third-party*** *shall be considered to be a provider of a high-risk AI system for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances: (a) they put their name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual arrangements stipulating that the obligations are otherwise allocated; (b) they make a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service in such a way that it remains a high-risk AI system pursuant to Article 6; (c) they modify the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service in such a way that the AI system concerned becomes a high-risk AI system in accordance with Article 6;*

- Recital (89) - ***Third parties*** *making accessible to the public tools, services, processes, or AI components other than general-purpose AI models, should not be mandated to comply with requirements targeting the responsibilities along the AI value chain, in particular towards the provider that has used or integrated them, when those tools, services, processes, or AI components are made accessible under a free and open-source licence. Developers of free and open-source tools, services, processes, or AI components other than general-purpose AI models should be encouraged to*

implement widely adopted documentation practices, such as model cards and data sheets, as a way to accelerate information sharing along the AI value chain, allowing the promotion of trustworthy AI systems in the Union.

The European Commission has published the following general sources of guidance on the AI Act:

- Information page AI Act - AI Act | Shaping Europe's digital future.
- European AI Office - European AI Office | Shaping Europe's digital future.
- Artificial Intelligence – Questions and Answers - Artificial Intelligence – Q&As.
- European AI Office – General-Purpose AI models in the AI Act – Questions & Answers.
- European Commission - AI Pact.

Article 96 of the AI Act stipulates that the Commission shall develop guidelines on the implementation of the AI Act with respect to specific topics. At the beginning of February 2025, the following guidelines were published:

- EC Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) based on Article 96(1)(b) AI Act, published on 4 February 2025 - Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act. | Shaping Europe's digital future
- EC Guidelines on AI system definition based on Article 96(1)(f) AI Act, published on 6 February 2025 -
- The Commission publishes guidelines on AI system definition to facilitate the first AI Act's rules application | Shaping Europe's digital future

The Commission published an Implementing Decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence: Register of Commission Documents - C(2023)3215. In May 2023, a technical report for the European Commission's Joint Research Centre was published on the 'Analysis of the preliminary AI standardisation work plan in support of the AI Act' (Soler Garrido, J., Fano Yela, D., Panigutti, C., Junklewitz, H., Hamon, R., Evas, T., André, A. and Scalzo, S., Analysis of the preliminary AI standardisation work plan in support of the AI Act. JRC132833).

At the beginning of 2025, a consultation will be launched by the AI Office within the framework of applied AI. The consultation will involve Member States, but also industry, academia and private citizens.

The AI Act becomes applicable on a staggered basis. There are also transitional arrangements for AI systems that had been placed on the market or put into service before certain dates. For example, the AI Act does not apply to operators of high-risk AI systems that have been placed on the market or put into service before 2 August 2026 (for Annex III AI systems) or 2 August 2027 (for Annex I AI systems), unless those systems are subject to significant change in design (in which case, the provisions would apply in full). The relevant dates of application are set out below.

Timeline	
12 July 2024	The AI Act was published in the Official Journal of the EU, triggering the dates for specific provisions in the Regulation becoming applicable.
2 February 2025	Prohibited practices ban applies (Chapter II). AI literacy rules apply (article 4).

2 May 2025	Codes of practice for general-purpose AI must be ready (article 56 (9)).
2 August 2025	National authorities designated (Chapter III Section 4). Obligations for General-purpose AI (GPAI) (Chapter V). Governance (at EU and national level) (Chapter VII). Confidentiality and penalties (other than in relation to gen-AI) (Chapter XII).
2 August 2026	Start of application of all other provisions of the EU AI Act (unless a later date applies below).
2 August 2027	High-risk categories listed in Annex I. General-purpose AI models placed on the market before 2 August 2025 (article 111).
2 August 2030	High-risk AI systems (other than those listed below), which have been placed on the market or put into service before 2 August 2026 and which are intended to be used by public authorities (article 111).
31 December 2030	Components of large-scale IT systems listed in Annex X, which have been placed on the market or put into service before 2 August 2027 (article 111).

On 17 December 2024, the European Data Protection Board adopted Opinion 28/2024 "on certain data protection aspects related to the processing of personal data in the context of AI models." These guidelines specifically focus on the question if/to what extent AI models, and notably General-Purpose AI Models, comprise personal data, as well as the lawfulness of personal data processing in this context.

In 2022, a proposal for a directive on adopting non-contractual civil liability rules to artificial intelligence (**"AILD"**) was published (link: eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0496).[85] On 11 February 2025, the European Commission published its 2025 work programme, listing the AILD for withdrawal. "No foreseeable agreement" on the proposal was cited as the reason for withdrawal. The AILD has not yet been officially withdrawn but the European Commission will formally notify the European Parliament and the Council of the European Union of its intention to withdraw the proposal and consult with these institutions about the proposed withdrawal.

5.2. Combination of technologies: DLT/Blockchain and AI

In the 2nd cohort some use cases combining DLT/Blockchain and AI technology were selected.

Apart from the fact that DLT/Blockchain solutions are increasingly combined with AI generated content in applications such as supply chain monitoring, verification and reporting, DLT/Blockchain solutions are also developed to support reliable & predictable AI through decentralized knowledge graphs.

This functionality to support reliable & predictable AI leads to questions if and to what extent the provisions of the AI Act are applicable to such use cases and how the use of such applications might facilitate/enhance the compliance with the AI Act by other actors, including in particular the obligations that apply to providers of high-risk AI systems in connection with

[85] A complementary impact assessment was published on 19 September 2024 by the European Parliamentary Research Service (link EPRS_STU(2024)762861_EN.pdf).

requirements for data (and data governance), record-keeping, transparency, accuracy, robustness, cybersecurity and post-market monitoring.

Many of these combined DLT/AI solutions are at least in part based on open-source AI systems or products as open-source is one of the corner stones for DLT. Therefore, the open-source provisions in the AI Act are of specific relevance for combined DLT/AI based solutions.

5.3. Regulation of open-source AI systems and AI products[86] in the AI Act

The AI Act contains specific provisions for *AI systems* and *AI Products* that are released under free and open-source licenses.[87] The AI Act does not apply to AI systems released under free and open-source licenses, unless they are placed on the market or put into service as high-risk AI systems or as an AI system that falls under Article 5 (prohibited AI practices) or Article 50 AI Act (transparency obligations for certain AI systems).[88] Furthermore, an exemption exists for certain responsibilities in relation to third-party providers of AI products that are integrated into high-risk AI systems, provided that such AI products are provided under a free and open-source license.

- Article 2(12) – **Scope** - *This Regulation does not apply to AI systems released under free and open-source licences, unless they are placed on the market or put into service as high-risk AI systems or as an AI system that falls under Article 5 or 50.*

- Article 25(4) AI Act – **Responsibilities along the AI value chain** - *The provider of a high-risk AI system and the third party that supplies an AI system, tools, services, components, or processes that are used or integrated in a high-risk AI system shall, by written agreement, specify the necessary information, capabilities, technical access and other assistance based on the generally acknowledged state of the art, in order to enable the provider of the high-risk AI system to fully comply with the obligations set out in this Regulation.* ***This paragraph shall not apply to third parties making accessible to the public tools, services, processes, or components, other than general-purpose AI models, under a free and open-source licence.*** [emphasis added]

Recital 103 of the AI Act makes a distinction between the provision of AI systems under “free and open-source licences" on the one hand and provision of such systems *against a price or otherwise monetised* on the other hand.

- Recital (103) - *Free and open-source AI components covers the software and data, including models and general-purpose AI models, tools, services or processes of an AI system.* ***Free and open-source AI components can be provided through different channels, including their development on open repositories.*** *For the purposes of this Regulation,* ***AI components that are provided against a price or otherwise monetised****, including through the provision of technical support or other services, including through a software platform, related to the AI component, or the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software, with the exception of transactions between microenterprises,* ***should not benefit from the exceptions provided to free and open-source AI components****. The fact of making AI components available*

[86] In this report the term ‘AI products’ is used to ensure that all relevant products are captured: (general-purpose) AI models and AI tools, services, components and processes which are integrated in AI systems.

[87] Articles 2(12), 25(4) and recital 103 AI Act.

[88] Paragraph 2.5.5. of the EC Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) based on Article 96(1)(b) AI Act, published on 4 February 2025.

through open repositories should not, in itself, constitute a monetisation. [emphasis added]

During the dialogue meetings, questions were raised in relation to the applicability of the aforementioned open-source exemptions as well as the allocation of responsibilities in the event of deployment or use of open-source AI systems or components between providers and third-party suppliers. Although no conclusions were reached, different aspects were identified that will be relevant for the assessment/allocation of legal responsibilities in relation to open-source AI systems or products, including the level of involvement of the provider of the AI product:

➢ **Relevant laws and regulations:**	➢ **Relevant characteristics** to determine the responsibilities of providers or third-party suppliers of (elements of) open-source AI systems (examples):
▪ Relevant provisions in the AI Act (Art. 2,. Art. 3, Art. 25) ▪ Contractual obligations (if applicable) ▪ Potentially relevant provisions in other national/EU legislation, such as (not exhaustive): o The GDPR, the e-Privacy Directive and the Law Enforcement Directive o Financial services law instruments referred to in Recital 158 AI Act o Revised Product Liability Directive (PLD) o Specific EU laws referred to in Annex I of the AI Act	▪ "Under a free and open-source licence" or "provided against a price or otherwise monetised"? To be assessed a.o. on the basis of the level of involvement of the provider of the AI Product. ▪ High risk AI system or other AI system? ▪ AI system or AI tools, services, components or processes? ▪ Used or integrated in a high-risk AI system or not? ▪ Provider or third-party supplier?

In **Annex II** to this report a high-level overview of legal obligations to offering AI systems and AI products provided "under free and open-source licenses" for providers and third-party suppliers is added.

5.4. Areas for further clarification & dialogue

Several areas for further clarification and regulatory dialogue were identified during the dialogue meetings.

5.4.1. Areas for deeper dives

The following areas for deeper dives into some of the topics that were discussed during the 2nd round of dialogues were identified:

- Is Article 25(4) AI Act applicable to third-party suppliers that are not in scope of the AI Act pursuant to Article 2(1) of the AI Act?[89] In other words: are the obligations included in Article 25(4) of the AI Act only addressed to the high-risk AI system provider and not to the third-party supplier who does not meet the applicability criteria of Article 2(1)?
- Are complete AI systems included in the exception for suppliers of open-source functionality referred to in Article 25(4) or is this exception limited to suppliers of tools, services, components or processes?

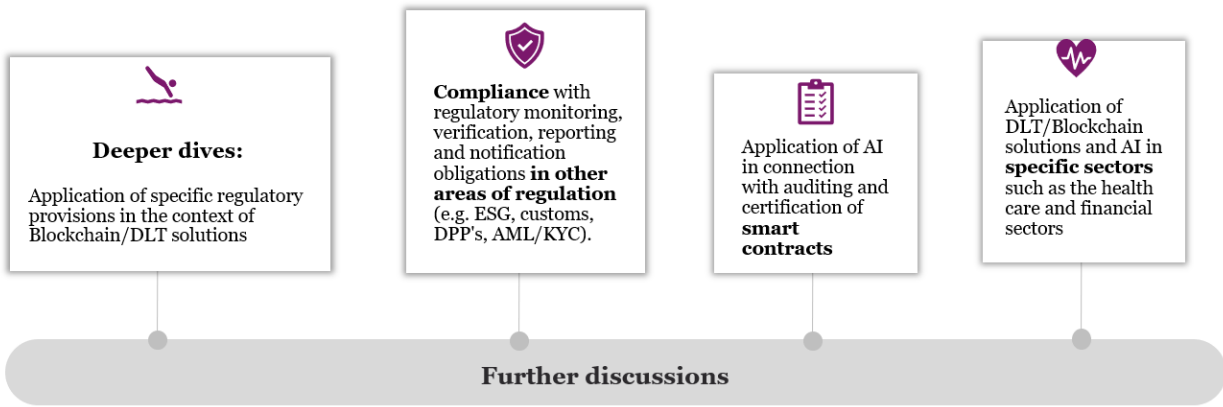
[89] Article 2 of the AI Act determines the scope of the applicability of the provisions of the Act. Third-party suppliers of AI Systems/Products are not mentioned among the categories in **Article 2(1) AI Act**: "*This Regulation applies to: **(a)** providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country; **(b)** deployers of AI systems that have their place of establishment or are located within the Union; **(c)** providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union; **(d)** importers and distributors of AI systems; **(e)** product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark; **(f)** authorised representatives of providers, which are not established in the Union; **(g)** affected persons that are located in the Union.*"

- What constitutes a modification or finetuning of a general-purpose AI model within the meaning of recital (109) of the AI Act?
- Who incurs obligations related to modification or finetuning when the blockchain use case provider is doing this on the instructions of the customer?
- Does the position change if the blockchain use case provider helps the customer with the integration of third-party general-purpose AI models (including if, for example, LLMs need to be quantised for the integration to incur in the way the user wishes)?
- Who incurs obligations related to high-risk AI systems or transparency risk AI systems (as included in Article 50) if the blockchain use case provider (further) develops such systems on the instructions of the customer?

5.4.2. Additional topics

In addition new areas/topics for further discussion were identified:

- The use of DLT/Blockchain solutions in combination with AI generated content for the purpose of compliance with regulatory monitoring, verification, reporting and notification obligations in other areas of regulation (e.g. ESG, customs, DPP's, AML/KYC).
- The application of AI in connection with the auditing and certification of smart contracts
- Application of DLT/Blockchain solutions and AI in specific sectors such as health care and the financial sector



6. Decentralised Autonomous Organisations (DAOs) – legal wrapper; GDPR compliance

6.1. Introduction

Regulatory compliance, including compliance with the GDPR, and civil liability in the context of a DAO were again important areas during this round of European Blockchain Sandbox dialogues.

Reference is made to Chapter 3 (GDPR) and 5 (DAO's) of the 1st cohort best practices report. In this section some parts of this report that served as a basis for the 2nd round of dialogues are quoted below in *blue*.

Summary of findings in the report[90]

- *A Decentralized Autonomous Organisation ("**DAO**") is not a defined term and is currently not used in EU legislation. There are different types of "DAOs": **with or without a legal wrapper** and **for-profit/non-profit**.*

- *Different* examples of published DAO-descriptions are included in the 1st cohort best practices report. The common denominators appear to be the use of distributed ledger technology such as blockchain and "decentralized governance" meaning that decision-making is distributed among multiple parties.

- *DAOs present a challenge to both national and Union legislation with respect to the incorporation, registration, existence and the application of and compliance with regulation of legal entities. DAOs as such are not recognized as a separate category of legal entities.*

- *At this point in time, DAOs are often registered in commercial registers through legal 'wrappers': registering a DAO through existing legal entities, mostly foundations or associations. This practice does exist in few European countries, such as Switzerland, Liechtenstein and Estonia. Registering DAOs as independent legal entities is not yet foreseen in any national law within Europe currently.*

- *DAOs operating on a distributed ledger system, without legal entity status and lacking a central authority figure, may be incompatible with certain existing legal frameworks which are designed to govern legal or natural persons. Thus, such DAOs (depending on their activities) may face compliance issues and pose a complex challenge for regulators due to their inherent conflict with traditional legal frameworks. At the same time individual DAO-members who operate without legal entity status may face complex regulatory and civil liability issues if something goes wrong.*

- *Legal entity status and a physical address of a DAO will therefore often be in the interest of all involved (including competent authorities) for reasons of regulatory compliance, civil liability issues and the possibility to "own" assets such as solar parks, IP rights etc.*

[90] Chapter 5 (DAO's – Commercial Registers, 1st cohort best practices report (June 2024).

The above findings in the 1st best practices report were confirmed during the 2nd round of dialogues.[91]

Legislation is currently not specifically designed for DAO's. The legal/regulatory analyses and where a DAO does dock in the real world will be tailormade on the basis of the nature of the DAO activities and if these activities are regulated.

Apart from regulatory compliance, civil liability issues for individual DAO members and/or initiators, in particular in relation to DAOs without legal entity status, deserve specific attention. Additionally, there is a tension between smart contracts deployed in a DAO context (which are self-executing and immutable) and traditional legal frameworks, which require interpretability and flexibility.

- Example: criminal law case in the Netherlands regarding the original initiator of a cryptocurrency mixer (anonymized software tool/smart contract that allows users to conceal the source or owner of digital assets), which is currently pending in appeal.[92]

These observations and findings support the conclusion that it is important for DAO's to find an appropriate legal entity that respects the main characteristics of the DAO but at the same time allows the DAO to comply with applicable legislation/regulations.

In general terms it should be noted that the DAO related regulatory topics are under development and dependent on national legislation/supervision. Therefore, an ongoing dialogue on EU and national level with relevant stakeholders will be needed.

6.2. Legal entity status

Summary of findings in the report[93]

- *Article 49 TFEU: If a legal entity is recognised in one Member State (either on the basis of the incorporation theory or on the actual seat theory), such legal entity should also be recognised as a legal entity in other Member States.*
- *The categories of legal entities are determined by national law or based on EU legislation such as for instance an EEIG (Regulation (EEC) No. 2137/85), an SCE (Regulation (EC) No. 1435/2003) or an SE (Regulation (EC) No. 2157/2001).*
- *Legal entities are governed by the national law of the Member State where they are established or by the national law of the Member state where they are incorporated:*
  - *If a legal wrapper is used: based on the national law governing the relevant legal entity*
  - *In other cases: depending on applicable national legislation*
- *Therefore, whether a DAO (either with or without a legal wrapper) is recognised as a legal entity is a matter of national law, but once it is recognised as a legal entity in one of the Member States, all other Member States are required to recognise the DAO as such. Whether a DAO is a legal entity requires a case-by-case analysis.*

---

91 After completion of the DAO focused dialogues ETSI published the document ETSI GR PDL 029 V1.1.1 (2025-02) regarding "Permissioned Distributed Ledger (PDL); Digital Autonomous Organization (DAO)". The document explores DAO's in the context of Permissioned Distributed Ledger systems and provides the following definition of a DAO: "Decentralized Autonomous Organization (DAO): system that enables distributed decision making, management and ownership of assets, typically operated on a Blockchain or distributed ledger technology": GR PDL 029 - V1.1.1 - Permissioned Distributed Ledger (PDL); Digital Autonomous Organization (DAO)

92 Judgment of Rechtbank Oost-Brabant (NL) of 14 May 2024 (ECLI:NL:RBOBR:2024:2069) (*Tornado Cash*).

93 Chapter 5, DAO's – Commercial registers, 1st cohort best practices report (June 2024).

There is no universally accepted legal personality for DAOs. Areas for further analyses that have been identified in the 1st cohort best practices report are if the European Cooperative Society ("SCE")[94] and the proposal for European cross-border associations ("ECBAs")[95] are or could become appropriate EU legal vehicles for respectively DAOs for profit and non-profit DAOs.

Proposed ECBA Directive (Proposal for a Directive on European cross-border associations):[96]

- Article 1 – Subject matter – Coordination of the conditions for establishing and operating EBCA's
- Article 12 - Member States shall ensure that an ECBA shall only be required to register once. Registration shall take place in accordance with Articles 18 and 19.
- Articles 18 & 19 – Registration requirements include a.o.: name, statutes, postal address, names/addresses authorised representatives
- Article 22 – Mobility – Member States shall ensure that an ECBA has the right to transfer its registered office from one Member State to another without the need for dissolution of the ECBA or the creation of a new legal person in the Member State to which its office is transferred.

SCE Regulation[97]

- Focus on establishing an SCE; less on operational phase
- Registration requirements in accordance with national registration requirements which may require different registration requirements and registration requirements in more Member States depending on national requirements
- Article 7 – Transfer of registered office of an SCE from one Member State to another requires that the SCE meets the national requirements of the Member State to which its office is transferred (which in practice requires dissolution and incorporating a new SCE)

6.3. Case study - Can DAO characteristics be facilitated by an SCE?

In the 1st cohort best practices report several characteristics (non-exhaustive) of an effective DAO have been identified which can serve as a checklist to "test" to what extent such characteristics can be facilitated by legal entities legislation. These characteristics have been further specified (2nd cohort additions in *italics*):

- Members with voting rights;
- A well-defined purpose which is aligned with the interest of the members;
- Distributed/multi stakeholder and transparent governance and interests (financial or non-financial); *often involving the issue of tokens that give the holders voting and governance rights and/or a treasury in the form of a fund often composed of various crypto-tokens held in smart contracts, used to support the organisation's operations*;
- Required organs for decision making and representation, including appointments and change of members;
- Decentralised/electronic decision-making, bookkeeping and administration;
- Limitation of liability of founders/individual members;
- Acceptance of the use of smart contracts for decision-making;
- Clear rules regarding representation vis-à-vis other market parties/authorities. And the power of intervention: who has the power to intervene when things are going wrong, while maintaining the decentralized aspect of the DAO;
- Rules for winding up a DAO.

---

94 Regulation (EC) No. 1435/2003.
95 Proposal of 5 September 2023 for a Directive on European cross-border associations (COM(2023) 516 final (link).
96 EC Proposal of 5 September 2023 (link); Outcome of the EP's 1st reading 2 July 2024: (link).
97 No 1435/2003 of 22 July 2003 on the Statute for a European Cooperative Society (SCE) (link).

In the course of the 2nd round of dialogues it could be discussed in more detail if/to what extent these characteristics can be accommodated by using an SCE as a legal wrapper for “for profit” DAO’s. Possible issues and solutions were identified in connection with the application of certain SCE requirements such as:

1) Formation
2) Well defined purpose which is aligned with the interest of the DAO members
3) Physical address
4) Formalities in connection with shares; can shares in an SCE be tokenized?
5) Distributed/multi-stakeholder and transparent governance and interests (financial or non-financial). Is it possible to use smart contracts for decision-making?
6) Required organs, including appointments and change of members; management board; internal decision making and external representation
7) Book-keeping and administration
8) Connection between founders and co-ownership (limitation of liability of founders/individual members)
9) Rules for winding up

The possible issues and solutions that have been identified during the dialogues are summarized in the table that is attached as **Annex III.**

In summary, although the use of an SCE as a legal wrapper could be an option and several DAO characteristics could be accommodated by an SCE (although the structuring for individual DAO's would need further consideration), there were also more fundamental challenges identified, notably:

- The need to appoint a management board taking management decisions which is at odds with the decentralised joint decision making by all members through smart contracts.

- In addition, the fact that members of the management board would likely have to register as UBOs and would be subject to liability claims for mismanagement, could make it difficult to find members of a DAO who would be prepared to take on this role as it would be contrary to the concept of decentralised decision making.

These issues are likely not typical for SCE's but connected with the concept of a commercially operating legal entity.

The above challenges could possibly be addressed by a new legal entity/structure that accommodates the basic features of a DAO including that decisions are jointly taken by the members/token holders while the external representation and associated liability for mismanagement are not resting with the individual DAO members.

6.4. GDPR compliance in the context of a DAO

The GDPR does not contain a specific regime for DAO’s. Nevertheless, the fact that DAO’s have as a common element a blockchain-based collaboration among individual natural persons (data subjects) means that the GDPR is normally a very relevant area.

Reference is made to [Chapter 3]. In addition, the following DAO specific observations were discussed.

Public permissionless blockchains: are allowed under the GDPR, provided that the requirements of the GDPR are complied with. The DAO data controller(s) need to be able to demonstrate compliance with the various obligations under the GDPR and especially in relation to data subject rights. More certainty regarding e.g. the qualification of the role of the

node operators and date subject rights in the context of public permissionless blockchains would be welcome.

Smart contracts: It is important to assess if the processing of data through smart contracts does result in decisions which are binding for the DAO Members and produce legal effects for the individual DAO Members. If the smart contract only results in an option while human intervention is always needed for a binding decision, applicability of Article 22 GDPR will be less likely.

Legal basis in de context of a DAO:
Often DAO members will (implicitly) accept the terms and conditions laid down in the smart contracts if they join the DAO ecosystem. The main question is if this qualifies as *"processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"* in the sense of Art. 6(1)(b) GDPR.

It depends on the smart contract if it qualifies as a legal contract under civil law or if it is just software code implementing an agreement (which under civil law does not even always need to be in writing). It is important to test if such a smart contract, that qualifies as a legal contract under civil law, meets the criteria of the GDPR which assumes a 'positive agreement' based on explicit and informed consent.

A solution could possibly be that Terms & Conditions are applied that are accepted by the DAO member including that the DAO member accepts the smart contract. If everything is properly explained in the Terms & Conditions in conformity with e.g. the right to information under the GDPR that could possibly work.

The short conclusion is that 'contractual necessity' as a legal basis will only apply if the smart contracts for the use case comply with the GDPR.

6.5. Areas for further clarification & dialogue topics for the next cohorts

Several areas were identified that could be discussed in more detail in the next round of dialogues including but not limited to:

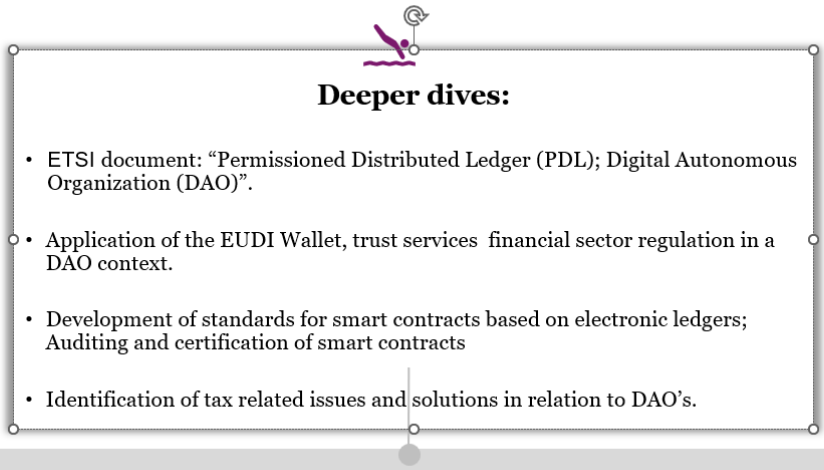
- The findings in the 2nd round of dialogues could be tested for DAO's with a different set-up and other regulated activities such as financial sector regulation. For non-profit DAO's the possibilities of an ECBA as a legal wrapper could be discussed.

- The application of regulatory instruments to DAO's with/without legal entity status could be tested such as the application of the EUDI Wallet and trust services regulated in the eIDAS2 regulation (2024/1183) and the application of existing financial sector regulation.

- Deeper dives in relation to the application of the GDPR in the context of public permissionless blockchains.

- Requirements for smart contracts and to what extent the essential requirements and standards for smart contracts in the Data Act are applicable.

- Identification of tax related issues and solutions in relation to DAO's.


Deeper dives:
• ETSI document: “Permissioned Distributed Ledger (PDL); Digital Autonomous Organization (DAO)”.
• Application of the EUDI Wallet, trust services financial sector regulation in a DAO context.
• Development of standards for smart contracts based on electronic ledgers; Auditing and certification of smart contracts
• Identification of tax related issues and solutions in relation to DAO’s.
Further discussions

7. Blockchain/DLT solutions for e-voting

7.1. Introduction

E-voting refers to the use of electronic means for voting and/or counting purposes. This includes e-voting machines in polling stations, the use of optical scanners to register and/or count paper ballots and remote e-voting (i.e., internet voting), which occurs outside the premises where voting would normally take place.

This definition, framed in the context of the Council of Europe's recommendation on standards for e-voting[98], encompasses various methods of electronic voting, ensuring a broad understanding of e-voting practices.

7.2. E-voting: Regulatory framework e-voting at EU level

The regulatory framework for e-voting at the EU level is shaped by a combination of national laws and EU (soft) legal instruments.

The **Current Consolidated Act of 20 September 1976**[99] sets the foundation for the election of European Parliament members. It mandates that elections must be based on proportional representation, conducted through direct universal suffrage, and ensure that voting is free and secret. Member States have the flexibility to authorize preferential list systems and are responsible for governing the electoral procedure, provided it maintains the proportional nature of the voting system.

In addition to these foundational rules, the **Council Decision (EU, Euratom) 2018/994**[100] allows Member States to offer advance voting, postal voting, and electronic/internet voting for European Parliament elections. These methods must ensure the reliability of the results, the secrecy of the vote, and the protection of personal data.

The **Compendium of E-voting and Other ICT Practices** highlights several critical considerations for implementing e-voting. It emphasizes the importance of addressing security risks, ensuring data protection, and maintaining inclusiveness. The introduction of e-voting should be accompanied by robust measures to ensure the process is secure and accessible to all voters, including those with disabilities.

The **Council of Europe Recommendation CM/Rec (2017)5** provides detailed standards for e-voting, focusing on principles such as universal suffrage, equal suffrage, free suffrage, and secret suffrage. These standards ensure that e-voting systems are user-friendly, secure, and maintain the integrity and secrecy of the vote. The recommendation also stresses the importance of transparency, accountability, and the reliability and security of e-voting systems.

Finally, the **Council of Europe CM(2022)10 Guidelines**[101] offer additional guidance on the use of ICT in electoral processes. These guidelines emphasize the need for ICT solutions to

---

98 Recommendation CM/Rec (2017)5 of the Committee of Ministers to Member States on standards for e-voting (adopted by the Committee of Ministers on 14 June 2017 at the 1,289th meeting of the Ministers' Deputies). (https://rm.coe.int/0900001680726f6f) Reference is also made to the Compendium of e-voting and other ICT practices, Directorate-General for Justice and Consumers, 6 December 2023. (https://commission.europa.eu/publications/compendium-e-voting-and-other-ict-practices_en)

99 Act concerning the election of the representatives of the Assembly by direct universal suffrage OJ L 278, 8.10.1976.

100 Council Decision (EU, Euratom) 2018/994 of 13 July 2018 amending the Act concerning the election of the members of the European Parliament by direct universal suffrage, annexed to Council Decision 76/787/ECSC, EEC, Euratom of 20 September 1976, OJ L 178, 16.7.2018.

101 Committee of Ministers Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States, CM(2022)10-final.

respect democratic principles, ensure usability and accessibility, and maintain the integrity and authenticity of electoral information. They also highlight the importance of continuous risk management, independent evaluations, and the ultimate responsibility of Member States in overseeing the use of ICT in elections.

Based on the Council of Europe's Guidelines on the use of information and communication technology (ICT) in electoral processes, e.g. the following areas of interest have been identified:[102]

- ensure that **ICT solutions respect the principles of democratic elections and referendums**, and that sufficient consideration is given to other relevant principles;
- ensure the **usability and the accessibility of ICT solutions** used in the electoral process by applying a human-centred approach;
- where an **e-solution is provided which is not universally accessible, an alternative**, broadly accessible **solution should also be provided**;
- ensure the **integrity and authenticity of the information provided by** ICT solutions used in the electoral process, procedures should be put in place to detect and, if possible, correct any errors or unauthorised intervention;
- ensure the **availability and reliability** of the ICT solutions used in the electoral process;
- ensure the **secrecy and confidentiality of information** stored within the ICT solution, as required by election and data-protection laws;
- ensure **transparency of the election and of the ICT solutions** used;
- organise an **evaluation of the ICT solutions** used in the election process by independent experts **prior to implementation**;
- conduct **continuous risk management** of the ICT solutions used in the election process;
- build and retain the **necessary capacity to assess, introduce and manage the use of ICT solutions** in the electoral process;
- **Member States should be ultimately responsible, also when private stakeholders are involved**; and
- **proactively address the possible use of ICT solutions in situations where "force majeure" affects the regular conduct of elections**.

7.3. E-voting: formal elections, referendums, consultation processes

Distinctions can be made between e-voting in formal elections, referendums, and consultations not governed by specific legislation, with varied applications and different regulatory frameworks governing electronic voting systems.

Formal Elections: E-voting in formal elections involves the use of electronic means to cast and count votes for official positions, such as members of parliament or local government officials. Countries like Estonia have integrated i-voting into their national legislation, allowing citizens to vote electronically using secure identification methods like eID cards (more on that

[102] Source: Council of Europe CM(2022)10 Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States (https://search.coe.int/cm?i=0900001680a575d9).

below). In contrast, countries like the Netherlands and Italy have either limited or no provisions for e-voting in formal elections, although experimental trials have been conducted.

Referendums: E-voting in referendums allows citizens to vote on specific issues or legislative changes. For example, the Netherlands is considering a constitutional amendment to introduce corrective referendums, which would involve a multi-step process requiring support from a minimum number of eligible voters. While e-voting for referendums is not yet widely implemented, it holds potential for increasing voter participation and accessibility.

Consultations: E-voting in consultations refers to the use of electronic means to gather public opinion on proposed decisions by public authorities. These consultations can be mandatory, as in the case of certain decisions governed by the General Administrative Law Act in the Netherlands, or voluntary, often organized via the internet. Consultations aim to involve interested parties in the decision-making process, ensuring transparency and inclusiveness.

The European Commission's Compendium of e-voting and other ICT practices provides several examples in Member States based on common knowledge but is not specifically focused on DLT based solutions but on different ICT practices.

7.4. E-voting: Regulatory framework and DLT based e-voting use cases at national level

The implementation and regulation of e-voting in formal elections varies significantly across different EU Member States, reflecting a range of approaches and experiences. Examples in Belgium, Portugal, France, Estonia, Ireland, Lithuania and Romania and Czechia are given in the Compendium of e-voting and other ICT practice of the Directorate-General for Justice and Consumers, 6 December 2023, some of which are briefly described below.[103]

7.4.1. Greece

In **Greece**, e-voting using blockchain is tested in the context of the municipal Youth Council in Trikala.[104] In January 2024, a small-scale deployment and validation was held in a controlled environment, which helped to fine-tune the system based on the feedback gathered through a dedicated questionnaire regarding TREVO usability, performance, security and user-friendliness. In March 2024, a large-scale deployment and validation was held in Trikala, which incorporated the full functionality of the system i.e. voter registration, election setup, voting, tallying of results and generation of voting (zero knowledge) proofs in the context of the municipal Youth Council. The Youth Council has specific monthly meetings and activities, and the members are very tech-focused which makes it very suitable as a test environment. The evaluation results are very positive.

7.4.2. Estonia

Estonia has gained very relevant experience in the area of electronic voting, having integrated it into the Estonian national legislation.[105] Chapter 7 of the Riigikogu Election Act[106] allows for electronic voting, which is administered by the State Electoral Office. For elections voters can still choose to vote in the traditional (paper) way. Estonia made history in 2005 by becoming the first country to allow its citizens to vote online in local elections. This innovation quickly expanded to include national and European elections. The trend of internet voting has steadily increased, with over 50% of votes being cast online in recent elections. Studies in Estonia indicate e-Voting does not affect voter decisions or increase participation if paper voting is also available.

In Estonia, there is no specific definition for e-voting; instead, the term iVoting (internet voting) is used. Estonia has been using iVoting for 20 years, with requirements outlined in the electoral

[103] https://commission.europa.eu/publications/compendium-e-voting-and-other-ict-practices_en.
[104] https://www.facebook.com/dsn.trikkaion.
[105] See https://commission.europa.eu/publications/compendium-e-voting-and-other-ict-practices_en.
[106] See Riigikogu Election Act–Riigi Teataja.

legislation. Citizens can vote from their chosen locations using applications available on different operating systems. Estonian citizens can use an eID card, mobile ID, or smart ID for identification, ensuring a high level of trust and security. Indeed, the system relies on Estonian electronic identity, with digital signatures equivalent to paper-based signatures. The voting application authenticates these signatures, and once the ballot box is finalized, all related procedures to check issues, double votes, etc., are done offline. Voters can vote multiple times, but only the last vote is counted.

Voter's choice is encrypted, and vote secrecy is guaranteed via a public-private key system, and all procedures are audited. Digital signing of the vote guarantees that the vote cannot be tampered with. Before the vote counting digital signatures and encrypted votes are separated to ensure the anonymity of the vote.

While no technology is prescribed, Estonia does not use blockchain/DLT technologies in their iVoting system; instead, the Estonian system, created in 2017, uses homomorphic cryptography. They aim to use post-quantum cryptography for enhanced security in the future.

More information on Estonia's electronic voting system can be found in the following book about e-voting in Estonia: https://skytte.ut.ee/en/content/book-about-e-voting-estonia. This book by Mihkel Solvak and Kristjan Vassil, titled "E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-2015)," examines the evolution of e-voting in Estonia over a decade. Published in collaboration with the Estonian State Electoral Office, the book delves into various aspects such as the spread of e-voting among the Estonian electorate, voting patterns, and the societal and political impacts of e-voting. Further information can also be found in the following materials:

- Internet Voting and Voter Turnout - https://www.valimised.ee/sites/default/files/2021-10/Internet%20Voting%20and%20Voter%20Turnout.pdf
- Trust in Estonian Internet Voting - https://www.valimised.ee/sites/default/files/2021-10/Trust%20in%20Estonian%20Internet%20Voting.pdf
- ODHIR Observer Mission in Estonia-https://www.osce.org/odihr/elections/estonia

7.4.3. Romania

In **Romania**, has not adopted e-voting legislation but uses several ICT solutions to improve the management of elections and increase their overall transparency.[107] These ICT solutions include: (i) the electoral register first used in the 2014 European Parliament elections; (ii) the system for monitoring turnout and preventing illegal voting (SIMPV); and (iii) a tabulation system to aggregate data (SICPV).

To guarantee data integrity a block-chain solution for SIMPV and SICPV transactions was implemented created by a coalition of public authorities and academic organizations which created a trust solution via blockchain for voting registration. The system uses a peer-to-peer architecture with nodes and an API layer 2 blockchains to increase trust. Blockchain infrastructure complements the existing voting system. The system is used for local and EU elections, with information transmitted in real-time to the European Blockchain Services Infrastructure (EBSI) as transactions with block numbers and hashes. More information can be found here[108].

[107] See https://commission.europa.eu/publications/compendium-e-voting-and-other-ict-practices_en

[108] https://www.bitget.com/news/detail/12560604372985; https://coingeek.com/romania-taps-blockchain-for-presidential-elections/.

Other examples of DLT based e-voting use cases **outside the EEA** are described in the Study on the Benefits and Drawbacks of Remote Voting (2018) commissioned by the European Commission.[109]

7.5. Relevance of eIDAS 2 regulatory instruments for (DLT based) e-voting applications in elections

E-voting is not regulated on an EU level. The question if and to what extent (DLT based) e-voting is accepted in elections depends on the national legislation on elections.

That being said, the eIDAS 2 regulation provides regulatory instruments that could become important regulatory enablers for e-voting applications such as the EUDI Wallet for secure identification and registration of voters, the regulation of trust services for electronic attestation of attributes and of trust services for electronic ledgers.[110]

It is important that the smart contracts that provide the functions in the election are audited and transparent. Guidance and recommendations for (harmonized) smart contract auditing under the eIDAS or other relevant regulatory frameworks would be very welcome.[111] There are currently no technical standards adopted by the European Standardization Organisations that specifically focus on smart contracts. ETSI and CENELEC have dedicated committees for DLT, blockchain and smart contracts.[112]

[109] A 2018 study commissioned by the European Commission covers internet voting, including the prospective use of blockchain. Link to study: fe09325d-9b4e-489c-9097-34018b6f3f8c_en; Page 171 The prospect of blockchain-based voting systems.

[110] See chapter 4 eIDAS.

[111] A working group was established in January 2024 by the ACPR and the AMF in France to explore the topic of smart contract certification in the event of future DeFi regulation which could be helpful also in the context of other applications. The document was published on 3 February 2025: The ACPR and the AMF publish the conclusions of the Working group on the certification of smart contracts and open a public consultation | Autorité de contrôle prudentiel et de résolution.

[112] After completion of the eIDAS 2 focused dialogues for the 2*nd* round ETSI published the draft working document ETSI TR 119 540 V0.0.6 (2025-02) titled *"Electronic Signatures and Trust Infrastructures (ESI); Standardisation requirements for Smart Contracts based on Electronic Ledgers"*: ETSI DRAFT TR 119 540v0.0.6-public.pdf. The draft document defines standardisation issues for Smart Contracts, as defined in the Data Act and based on Electronic Ledgers as defined by eIDAS 2.

8. Blockchain/DLT solutions enhancing CSRD compliance

8.1. General Framework

8.1.1. CSRD

The 'Corporate Sustainability Reporting Directive' (**CSRD**)[113] is aimed at enhancing the transparency and consistency of (mandatory) sustainability reporting. The CSRD applies to both listed and non-listed large companies/large groups (within the meaning of Article 3(4) and Article 3(7) Accounting Directive 2013/34 (AAD), and to listed 'small and medium enterprises' (SMEs). Moreover, the CSRD applies also to non-EU-based ultimate parent undertakings of global groups with significant market presence in the EEA. The CSRD's reporting obligations take effect in stages, as clarified in the below overview of the categories of in-scope undertakings and their thresholds as well as the year in the reporting obligations become applicable:

Category	Criteria	Applicability
Listed EU-based large undertakings/large groups (already subject to the NFRD)[114]	• A balance sheet/asset total of at least EUR 25 million • Net sales of at least EUR 50 million; • More than 250 employees	Financial years starting on or after **1 January 2024**; companies concerned report in **2025** for **2024**
EU-based large undertakings/large groups	• A balance sheet/asset total of at least EUR 25 million • Net sales of at least EUR 50 million; • More than 250 employees	Financial years starting on or after **1 January 2025**; companies concerned report in **2026** for **2025**
Listed SMEs	• A balance sheet/asset total of at least EUR 5,000,000 • Net sales of at least EUR 10,000,000 • More than 50 employees;	Financial years starting on or after **1 January 2026**; companies concerned report in **2027** for **2026** (opt-out until 2028)
Non-EU-based companies	• Net sales above €150 million in the EU over two previous years, and; • OneEU-based large undertaking/large group **or** • Branch with a turnover of more than EUR 40 million	Financial years commencing on or after **1 January 2028**; affected companies report **2028** for **2027**

In-scope companies are required to disclose information on their sustainability practices to ensure that their stakeholders are well-informed about the company's 'environmental, social, and governance' (**ESG**) activities. Particularly, the information to be reported encompasses ESG data of the undertaking's own operations as well as its upstream and downstream value chain, which includes its products and services, business relationships, and supply chain, under the so-called double materiality concept.[115]

[113] Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting (''**CSRD**'').

[114] Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups ("**NFRD**").

[115] Articles 19(a)(3) and 29(a)(3) CSRD.

The sustainability report needs to be prepared in accordance with the CSRD and the 'European Sustainability Reporting Standards' (**ESRS**).[116] Subsequently, the sustainability report must be verified by an independent assurance provider.[117] Member States thereby have the option to also allow a statutory auditor or audit firm other than the one(s) carrying out the statutory audit or an independent assurance services provider established in their territory that meets certain criteria.[118] The independent auditor or independent assurance services provider must assess and verify the accuracy and completeness of sustainability reporting by the company which involves the company's processes, controls, and data related to their ESG practices in accordance with the CSRD and the ESRS.

In August 2024 a draft Commission Notice was published with a set of Frequently Asked Questions (FAQs) which clarifies the interpretation of certain provisions on sustainability reporting introduced by the CSRD into the Accounting Directive (Directive 2013/34/EU), the Audit Directive (Directive 2006/43/EC), the Audit Regulation (Regulation (EU) No 537/2014), and the Transparency Directive (Directive 2004/109/EC) with the aim of facilitating their implementation by undertakings (CSRD FAQs). The FAQs also clarify certain provisions of the Sustainable Finance Disclosures Regulation "SFDR" (Regulation (EU) 2019/2088) and a limited number of clarifications concerning the interpretation of certain provisions of the ESRS (see next paragraph) where legal interpretation from the Commission has been deemed to be necessary. In addition, the Commission is working on a set of FAQs on the EU Taxonomy Delegated Acts. The FAQs will cover clarifications on the technical screening criteria for economic activities adopted in the Climate and Environmental Delegated Acts, as well as certain questions on the Disclosure Delegated Act. The FAQs are part of the Commission's efforts to enhance the usability of the EU Taxonomy. Further information about the EU taxonomy for sustainable activities can be found here: EU taxonomy for sustainable activities - European Commission.

As a 'Directive' within the meaning of Article 288 TFEU, the provisions of the CSRD must be transposed into the national legal system of the EU Member States. Additional reporting requirements, e.g. in relation to the scope of the reporting obligations but also on the required assurance reporting, could be imposed by the induvial Member States.

8.1.2. ESRS

The ESRS are a set of sustainability reporting standards determined by the Commission in accordance with Article 29b of Directive 2013/34/EU to support the implementation of the CSRD. The ESRS covers a wide range of sustainability topics, including but not limited to climate change, biodiversity, pollution, circular economy, human rights, and social issues. Currently, only the general ESRS have been published. The Commission still needs to adopt the sector specific ESRS and the ESRS for third country companies, which it has scheduled for 30 June 2026 at the latest.

At the request of the European Commission, the 'European Financial Reporting Advisory Group' (**EFRAG**) developed guidance to support companies with effectively complying with the general ESRS standards, thus promoting transparency and consistency in sustainability

[116] Commission Delegated Regulation (EU) 2023/2772 of 31 July 2023 supplementing Directive 2013/34/EU of the European Parliament and of the Council as regards sustainability reporting standards (''ESRS'').

[117] To this extent, the CSRD also amends the Transparency Directive and the Statutory Audits Directive.

[118] Article 34(4 & 5) Accounting Directive 2006/43/EC; note that Article 2(20) Accounting Directive: *"independent assurance services provider" means a conformity assessment body accredited in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council (*) for the specific conformity assessment activity referred to in point (aa) of the second subparagraph of Article 34(1) of this Directive."* (*) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).'

reporting.[119] On 31 May 2024, EFRAG published three ESRS 'Implementation Guidance' (**IG**) documents:

- IG 1: Materiality Assessment Implementation Guidance (MAIG)
  - Provides an illustrative materiality assessment process for undertakings and contains FAQs on the double materiality assessment to provide practical implementation guidance on disclosing material impacts, risks and opportunities.
- IG 2: Value Chain Implementation Guidance (VCIG)
  - Outlines the reporting requirements for the value chain from materiality assessment to policies and actions to metrics and targets. It illustrates the reporting boundary of the group for sustainability reporting, including the concept of operational control in environmental standards. The VCIG also includes FAQs for further information and a 'value chain map' summarising value chain implications per disclosure requirement across all ESRS.
- IG 3: List of ESRS Datapoints
  - Translates the complete ESRS Set 1 list of detailed requirements in each Disclosure Requirement and related Application Requirements in Excel format. The file contains additional information, such as the types of requirements (for example, quantitative or qualitative) or whether these are subject to transitional provisions. This list can form the basis for a data gap analysis or data collection exercise.

8.1.3. Regulatory Update February-April 2025

On February 26th, the Commission published its so-called Omnibus-I package for simplification and ease of ESG reporting obligations on business.[120] Whilst the Commission does not propose to amend the reporting obligations under CSRD, it does propose to amend the scope of the CSRD to EU-based companies with more than 1,000 employees. If accepted, this means sustainability reporting will no longer become mandatory for approx. 80% of the companies currently in scope of the CSRD. In addition, the Commission has announced a revision of the ESRS to (significantly) reduce the number of data points and abandonment of the application of sector-specific ESRS. In parallel, to create time for significant revision of the CSRD, the Commission separately proposed to the European Council and Parliament to postpone the application of the CSRD to large undertakings, large groups and listed SME's by 2 years.

On April 3rd, the European Parliament followed the Council in adopting the Commission's first proposal of the Omnibus-I package (to 'stop the clock') with overwhelming majority. This means that the application of CSRD for the 2nd and 3rd wave of in-scope companies will be delayed by 2 years giving the EU institutions time and space to consider the material proposal of the Omnibus package - the proposed material revision or 'simplification' of the CSRD.

Whatever may be the outcome of the discussions on these proposed changes, it is not expected to alter the supervision by national regulatory authorities nor the application of DLT/blockchain solutions supporting compliance with the CSRD regulatory framework.

8.1.4. The Sustainability statement

Article 19a(1) CSRD requires in-scope companies to include sustainability information in the management report to understand the undertaking's impact on sustainability matters as well as how sustainability matters affect the concerned undertaking (commonly referred to as the '*double materiality principle'*). To effectively comply with the CSRD's sustainability reporting obligation, ESG data must be collected, monitored, reported, and be verifiable. This is

[119] See the EFRAG ESRS Q&A platform: https://www.efrag.org/lab7 and its recently compiled overview of FAQ: https://www.efrag.org/Assets/Download?assetUrl=/sites/webpublishing/SiteAssets/Explanations+January+-+May+2024+%28final+version%29.pdf.

[120] For a summary of the main proposals, see https://www.twobirds.com/en/esg-pulse/shared/insights/2025/omnibus-i--simplifying-or-overhauling-the-eus-sustainability-regime.

important as the CSRD requires consistent measuring, monitoring, and reporting in order to enable an independent assurance provider to audit and provide an assurance opinion over the reporting.[121]

The CSRD requires mandatory assurance of the sustainability reporting by 'independent assurance providers', which must comply with the Commission's assurance standards that are adopted through the means of delegated acts.[122] Following the CSRD's amendment of the Accounting Directive 2013/34 (AAD), Article 34(1)(aa) AAD provides that independent assurance providers, which can be statutory auditors or audit firms,[123] shall also express an opinion based on compliance of the sustainability reporting with the ESRS, the process carried out by the undertaking to identify the information reported pursuant to those ESRS, and the compliance with the requirement to mark-up sustainability reporting in accordance with Article 29d CSRD.

Regarding the information that needs to be obtained, the CSRD requires that the ESG data used for sustainability reporting purposes must be relevant, comparable, and reliable.[124] The concerned information (both qualitative and quantitative information) must also meet the criteria by the ESRS.[125] Appendix B of ESRS I provides that the qualitative characteristics of information presented in the sustainability statement must be:

- Relevant;
- Faithfully representative;
- Comparable;
- Verifiable; and
- Understandable.

Sustainability information must be traceable, comparable, and machine-readable in digital formats.[126] The CSRD, therefore, requires single electronic reporting to be prepared in 'Extensible Hypertext Markup Language; (**XHTML**) format.[127] Furthermore, 'eXtensible Business Reporting Language' (**XBRL**) is required as inline. XBRL is machine-readable and allows for the automated consumption of large amount of information.[128] This enables the so-called digital tagging (or markup) of the reported ESG data in order to ensure this data can be accurately analysed and compared. Blockchain solutions that support document processing normally can support the storage of large files (> 1MB) in large quantities with scalable storage solutions and therefore can provide for reporting in this format. In parallel, ESMA is tasked with preparing the Regulatory Technical Standard (RTS) for a European Single Electronic Format (ESEF) as the standard for sustainability statements to be prepared in a human-readable format and a machine-readable format.[129]

EFRAG has been tasked by the European Commission to develop the digital XBRL taxonomy for the ESRS. In August 2024, EFRAG published the ESRS Set 1 XBRL Taxonomy, which describes requirements, standards and methods for the digital tagging of ESRS disclosures under the CSRD to allow "digital tagging" of the content of (ESRS) disclosures.

[121] Rec. 4, 13, 65-66 CSRD.
[122] Articles 26a(1) and 28a(1) CSRD.
[123] Member States may also appoint other independent assurance providers.
[124] Rec. 2 CSRD.
[125] Article 29b(1)(3) CSRD.
[126] Rec. 55 CSRD.
[127] Article 29d(1) CSRD, in conjunction with Article 3 Article 3 EC Delegated Regulation (EU) 2019/815.
[128] Rec. 4 Commission Delegated Regulation 2018/815.
[129] The consultation on the draft ESEF RTS for sustainability reporting by ESMA closed on 31 March 2025, see: Consultation on the ESEF RTS for sustainability reporting and on the amendments to the EEAP RTS.

8.1.5. Appointment and the role of national competent authorities

The CSRD does not mandate which competent authorities should be appointed by Member States for monitoring and enforcing sustainability reporting requirements. Nor does it stipulate what the remit of its competences should be or the consequences of non-compliance. The CSRD only requires that national competent financial regulatory authorities are being tasked with supervising and enforcing the sustainability reporting requirements for listed undertakings because these companies already fall under their financial regulatory supervision.[130] Furthermore, Member States must designate a national competent authority for supervising statutory auditors and audit firms with regard to the assurance of the sustainability reporting.[131]

Hence, it remains to the discretion of the Member States to also designate a national competent authority for supervising and enforcing the sustainability reporting obligation to non-listed in-scope undertakings.

8.2. Best practices, lessons learned

8.2.1. Key question: to what extent can DLT/blockchain solutions enhance compliance with CSRD reporting obligations?

In relation to how the information must be collected, assessed and audited, the CSRD is technology-neutral and does not exclude DLT/blockchain solutions as long as these applications comply within the parameters of the CSRD.

The CSRD regulatory framework regarding sustainability reporting and examination does not preclude the use of blockchain applications for the collection, processing and reporting of sustainability data and information to the competent authorities assuming that the information can be verified by an independent auditor or – if allowed by national legislation - an independent assurance services provider. In view of the fact that the data come from different (decentralized) sources and the Blockchain characteristics (e.g. possibilities to ensure integrity, immutability, transparency, tamper proofness) DLT/blockchain solutions could be very suitable for the different stages of reporting, which can be divided into collecting, monitoring, and reporting.

Standards are highly relevant for the application of blockchain/DLT based solutions that aim to support compliance with the CSRD regulatory framework. It is important that the standards that are developed do not unnecessarily limit the application of such solutions. On the one hand it is important that standards in connection with the use of Blockchain/DLT solutions become available in time and provide enough certainty to enhance investments and market adoption and on the other hand too much detail that could hamper new developments and solutions has to be avoided. Another important element is that the standards should facilitate scalability in view of the fact that the scope of the sustainability reporting requirements will be broadened.

How the sustainability data are collected is important, but supervision also needs to focus on the process of collecting and reporting of sustainability data and information. The reporting of sustainability data on the basis of the CSRD regulatory framework is the task of the regulated entities. If the Blockchain/DLT solution works for these regulated entities (and their independent auditor/assurance service provider), the competent authorities will still need to do their examination.

8.2.2. Guidance to national competent authorities

Regulatory enforcement and supervision of the CSRD is, in principle, only mandatory for listed large undertakings or large groups and listed SMEs.[132] Following its amendment by the CSRD,

[130] Recs. 57, 79 CSRD.
[131] Articles 30, 30a(3), and 31(2) of the consolidated Transparency Directive.
[132] Also known as undertakings whose securities are admitted to trading on a regulated market in the Union.

Article 4(4) of the Transparency Directive[133] requires national competent authorities to ensure that listed companies comply with corporate reporting requirements (including the sustainability reporting requirements laid down in the CSRD).[134]

Nevertheless, the guidance offered to and by the concerned regulatory authorities can provide insightful information with regard to the CSRD's technical and data collection requirements in general.

As listed undertakings are generally supervised by financial regulatory authorities, the European Securities and Markets Authority (ESMA) is required under the CSRD to issue guidelines for the competent supervisory authorities in the Member States to enhance consistent and effective supervision of sustainability reporting by issuers subject to the Transparency Directive.[135] On 15 December 2023, ESMA published the draft Guidelines on Enforcement of Sustainability Information ("**GLESI"**) and it expects to publish the final GLESI in Q3 2024.[136] The GLESI will apply to supervision and enforcement of the CSRD relating sustainability reports published from 1 January 2025.

The enforcement in scope of the GLESI relates to both:

- the sustainability information required by the Accounting Directive along with the ESRS and
- the sustainability information required by Article 8 of the Taxonomy Regulation[137] along with the Disclosures Delegated Act.[138]

According to draft Guideline 8 of the GLESI enforcers can use four different approaches when they examine sustainability information, differing on two parameters: whether the enforcer communicates with the issuer during the examination (interactive vs. desktop examination) and whether the enforcer bases its examination on the entirety or a subset of the sustainability information (unlimited vs. focused examination):[139]

> ***Guideline 8: Types of examination***
>
> *Enforcers should identify the most effective way to enforce sustainability information. As part of the ex-post activities regarding enforcement of sustainability information of issuers selected for examination, enforcers can use:*
>
> *a) interactive unlimited examinations,*
> *b) interactive focused examinations,*
> *c) desktop unlimited examinations, and*
> *d) desktop focused examinations.*

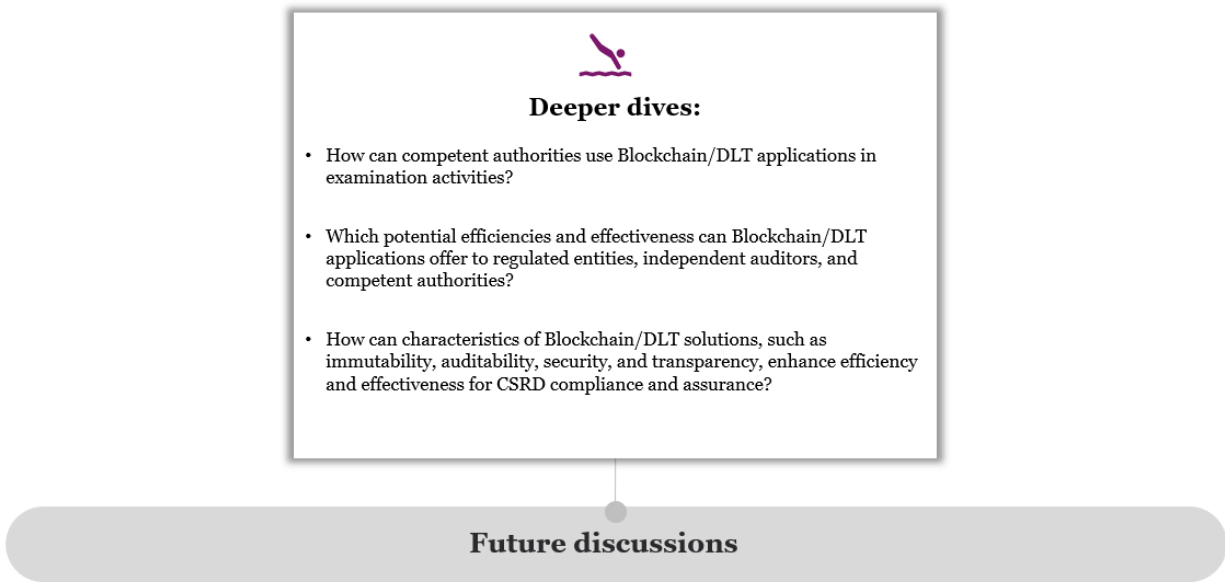
[133] Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC.
[134] Rec. 79 CSRD.
[135] Art. 28d Transparency Directive.
[136] Consultation Paper on Draft Guidelines on Enforcement of Sustainability Information (europa.eu).
[137] Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020 on the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088, OJ L 198, 22.6.2020, p. 13–43.
[138] Commission Delegated Regulation (EU) 2021/2178 of 6 July 2021 supplementing Regulation (EU) 2020/852 of the European Parliament and of the Council by specifying the content and presentation of information to be disclosed by undertakings subject to Articles 19a or 29a of Directive 2013/34/EU concerning environmentally sustainable economic activities, and specifying the methodology to comply with that disclosure obligation, OJ L 443, 10.12.2021, p. 9–67.
[139] This Draft Guideline is based on Guideline 6 of the GLEFI. ESMA is proposing that no substantial changes are needed compared to the GLEFI text (Draft GLESI, par. 52).

According to ESMA's final report on the GLESI consultation,[140] respondents mostly agreed with these types of examination.

8.2.3. Areas for further clarification & dialogue topics for the next cohorts

Several areas for further investigation and analyses were identified:

- How could Blockchain/DLT applications also be used by competent authorities as part of their examination activities in accordance with the GLESI and what would it mean from an operational point of view.
- If/how can Blockchain/DLT applications be used to gain efficiencies/effectiveness for regulated entities, independent auditors/independent assurance services providers and the competent authorities.
- How can the characteristics of Blockchain/DLT solutions such as immutability, auditability, protection against tampering, security, differentiated access and transparency be used to enhance efficiency/effectiveness of compliance with the CSRD regulatory framework (including not only collecting the right data but also ensuring a reliable process) and how can this be supported in the applicable standards.



[140] On 5 July 2024 ESMA published its final report on the consultation: https://www.esma.europa.eu/sites/default/files/2024-07/ESMA32-992851010-1600_Final_Report_on_Guidelines_on_Enforcement_of_Sustainability_Information_GLESI.pdf.

9. Blockchain/DLT solutions enhancing compliance with the EUDR and the interplay with horizontal Data Regulation

9.1. Introduction – the EU Deforestation Regulation (EUDR)

As part of the EU Green Deal, as well as the broader EU strategy to protect the world's forests, the EUDR[141] aims to "ensure that a set of key goods placed on the EU market will no longer contribute to deforestation and forest degradation in the EU and elsewhere in the world. Deforestation and forest degradation are important drivers of climate change and biodiversity loss — the two key environmental challenges of our time."[142] "Deforestation" means the conversion of forest to agricultural use, whether human-induced or not.[143] In addition, the EUDR aims to reduce the EU's contribution to greenhouse gas emissions and prevent global biodiversity loss. To achieve its purpose, the EUDR only allows deforestation-free commodities and products on the EU market, if these products are in-scope.

The material scope of the EUDR encompasses particular commodities identified in Article 2(1) EUDR, namely: cocoa, coffee, palm oil, soy, wood, cattle, and rubber. This list can be extended following the EUDR's review by the Commission after a period of two years). In addition, products that are being derived from these commodities and are listed in Annex 1 EUDR fall also within the scope of the EUDR.

Relevant EUDR data related requirements include:

- For operators/traders: analyses of supply chains, due diligence obligations, data collection, data storing, data sharing and reporting obligations.
- For regulators and authorities: Mandatory examination of documentation and records; information sharing between the EC, competent authorities and customs authorities

The EUDR applies to large 'operators' (those who place the listed product or relevant commodity on the EU market for the first time) and 'traders' (those who make the listed product or relevant commodity further available to the market). The EUDR applies to these market participants, regardless of the location of their legal establishment and their legal form. However, a special (less stringent) regime applies to 'small and medium-sized enterprises' (SMEs).

Operators and traders may mandate an authorized representative to submit due diligence statements on their behalf.[144]

The EUDR provides that in-scope products or commodities cannot be placed on the EU-market, unless they are deforestation-free, legally produced; and accompanied by a 'Due Diligence Statement' (DDS). Regarding this DDS, the EUDR outlines three main steps for compliance:

- gather geographic data, such as satellite imagery;
- assessing the risk of non-compliance with the EU deforestation-free standards pursuant to Article 10(2) EUDR;

[141] Regulation (EU) 2023/1115 of the European Parliament and of the Council of 31 May 2023 on the making available on the Union market and the export from the Union of certain commodities and products associated with deforestation and forest degradation and repealing Regulation (EU) No 995/2010 ("EUDR").

[142] Commission Notice guidance document for Regulation (EU) 2023/1115 of 13 November 2024 on deforestation-free products (C/2024/6789) (Link).

[143] Article 2(3) EUDR.

[144] Article 6 EUDR and the definition of Authorised representative in Article 2(22) EUDR.

- implementing measures to mitigate identified risks to negligible levels.

In December 2024 the EU granted a 12-month additional phasing-in period[145] making the law applicable on 30 December 2025 for large and medium companies and 30 June 2026 for micro and small enterprises.

The Commission has set up and manages a portal interface (information system – Art. 33 EUDR) to support operators and competent authorities in presenting and accessing information pursuant to the EUDR. Operators, traders or authorized representative should submit their due diligence statements through this portal. The information system is accessible to competent authorities and customs authorities and facilitates the transfer of information between Member States, competent authorities and customs authorities.

At this moment, the EUDR portal interface is already operational and allows for the voluntary submission of statements. There is a standardized API that companies can use to submit statements automatically. However, the main interoperability challenges lie in the traceability along the value chain.

9.2. Interplay with the UN Transparency Protocol and Recommendation 49

In May 2023, the United Nations Centre for Trade Facilitation and Electronic Business launched the project titled “Transparency at scale – digital solutions for trust, resilience and sustainability: verifiable credentials in supply chains”. Among the deliverables of this project is Recommendation No. 49, which will offer policy guidance on the implementation of traceability and transparency at scale through digital instruments, such as the United Nations Transparency Protocol for Digital Product Passports.

There is currently not a formal connection between the EUDR and the UN Transparency Protocol Initiative and the related Recommendation 49 but there is an informal working relationship (through working groups with participants of governments (EU/non-EU), small/big companies, service providers and other experts).

- Link to the Recommendation 49 Working Group activities and related: Draft Recommendation No. 49: Transparency at Scale | UNECE
- Link to become UNECE – UN/CEFACT Expert and participate to the Working Groups: UNCEFACT Expert Registration

Solutions that are being developed in the UNTP/Recommendation 49 working groups are actually already deployed in practice by different providers to gain experience (Software Solutions | UN Transparency Protocol). The companies participating in the working group that pledge the further developments are listed on this site.

On the basis of the discussions held in the 2nd cohort dialogues, Blockchain/DLT applications that deploy the aforementioned UNTP/Recommendation 49 solutions could support EUDR compliance. As mentioned above, the main interoperability challenges lie in the traceability along the value chain. This is one of the important topics in the recent UNECE consultation (the consultation term closed on 23 March 2025). The consultation documents can be accessed using this link: Public Review 2: Recommendation No. 49: Transparency at Scale.

[145] Regulation (EU) 2024/3234 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2023/1115 as regards provisions relating to the date of application.

9.3. Interplay between the EUDR and horizontal EU data regulation

The horizontal data regulation instruments and the sector- and domain-specific initiatives focused on data sharing are part of the European Single Market for Data as visualized in the scheme below.[146]

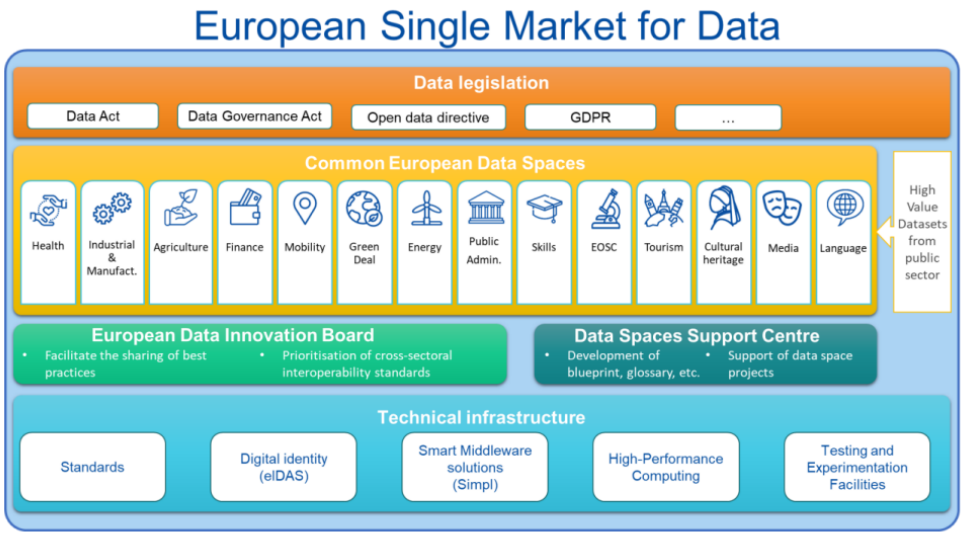


Figure 1 European single market for data (European Commission)

Depending on the characteristics of the DLT use case the provisions regarding data sharing/access, switching between (data) processing services and interoperability in sectoral and domain-specific EU legislation (such as the EUDR) and in horizontal EU data regulatory instruments such as the Data Act, the Data Governance Act and the Digital Services Act may apply in parallel.

9.4. Standardisation and interoperability in the Green Deal Data Space, including the EUDR

Chapter VIII of the Data Act[147] lays down obligations to ensure interoperability between participants in "Data Spaces" as well as obligations to ensure in-parallel use of data processing services and interoperability of data processing services.

The EC is working on the EU trusted data framework standards. The Data Act does provide a basis for creating a standard for common European Data Spaces in the interoperability chapter.[148]

> **Article 2(40) Data Act – definition of "interoperability"**
>
> *(40) 'interoperability' means the ability of two or more data spaces or communication networks, systems, connected products, applications, data processing services or components to exchange and use data in order to perform their functions;*

A draft standardization request of 5 November 2024 as regards the European Trusted Data Framework with references to the Staff Working Documents regarding common European data

---

[146] Source: HLF Workstream 14 on Data Interoperability – Final Report of 11 April 2024 (HLF Workstream 14 on Data Interoperability – Final Report).

[147] Articles 33 – 36 Data Act.

[148] Chapter VIII, Article 33(4) Data Act.

spaces (Link SWD 2022 and Link SWD 2024) as well as the Data Governance Act, the Data Act and several other regulatory instruments and documents is published here: DocsRoom - European Commission. The standardization request of 5 November 2024 is still a draft, but there will be a formal request going to the European standardization bodies (ETSI/CEN/CENELEC), with a deadline. When the groups are set up, usually there is then a call for interested companies to join.

For innovation and the further development of use cases in the Green Deal Data Space (including the EUDR) it is important that the standards that are adopted/developed under different regulatory instruments are consistent and take into account the standards that are already in place. Although no specific issues for Blockchain/DLT technology are expected, this is something to monitor.

9.5. Data Act - Qualification of Blockchain/DLT applications for ESG monitoring and reporting as "data processing services"?

The Data Act lays down obligations for data processing services. Chapter VI of the Data Act[149] contains obligations for providers of data processing services to facilitate switching between data processing services.

The terms "data processing service" and "switching" are defined in Article 2(8) and 2(34) of the Data Act:

> **Article 2(8) and 2(34) Data Act – definitions "data processing service" and "switching"**
>
> *(8) 'data processing service' means a digital service that is provided to a customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction;*
> *(34) 'switching' means the process involving a source provider of data processing services, a customer of a data processing service and, where relevant, a destination provider of data processing services, whereby the customer of a data processing service changes from using one data processing service to using another data processing service of the same service type, or other service, offered by a different provider of data processing services, or to an on-premises ICT infrastructure, including through extracting, transforming and uploading the data;*

According to Article 23 Data Act providers of "data processing services" as defined in the Data Act shall take measures to enable customers to switch to a data processing service, covering the same service type, which is provided by a different provider of data processing services, or to on-premises ICT infrastructure, or, where relevant, to use several providers of data processing services at the same time in accordance with the relevant provisions of the Data Act:

> *"In particular, providers of data processing services shall not impose and shall remove pre-commercial, commercial, technical, contractual and organisational obstacles, which inhibit customers from:*

[149] Articles 23 – 31 Data Act.

(a) *terminating, after the maximum notice period and the successful completion of the switching process, in accordance with Article 25, the contract of the data processing service;*
(b) *concluding new contracts with a different provider of data processing services covering the same service type;*
(c) *porting the customer's exportable data and digital assets, to a different provider of data processing services or to an on-premises ICT infrastructure, including after having benefited from a free-tier offering;*
(d) *in accordance with Article 24, achieving functional equivalence in the use of the new data processing service in the ICT environment of a different provider of data processing services covering the same service type;*
(e) *unbundling, where technically feasible, data processing services referred to in Article 30(1) from other data processing services provided by the provider of data processing services."*

Whether the obligations regarding switching between data processing services in the Data Act are applicable to Blockchain/DLT solutions will depend on the characteristics of the use case. The provisions of Chapter VI Data Act will likely not apply to blockchain/DLT use cases that act as a Data Intermediary Services merely using digital services/cloud services and not providing such services:[150]

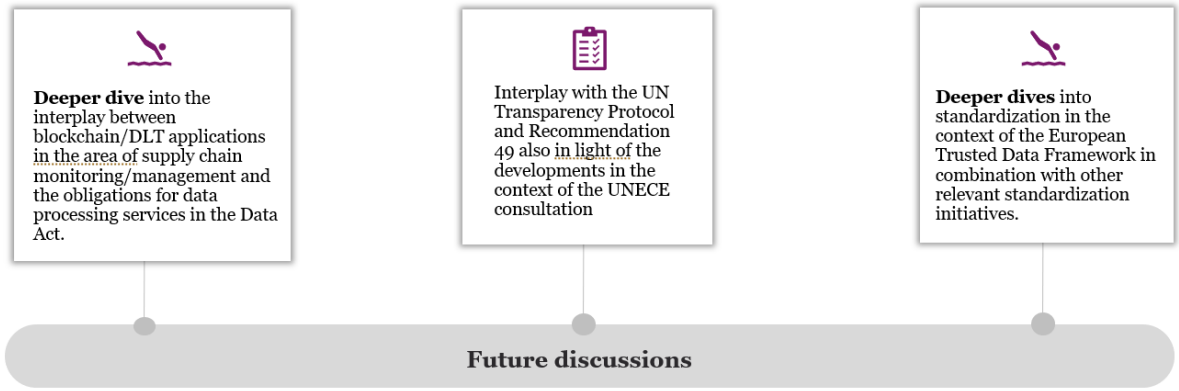
- Article 1(7) Data Act: "*This Regulation complements the self-regulatory approach of Regulation (EU) 2018/1807 by* ***adding generally applicable obligations on cloud switching****."*
- Data Act, recital (80): *"Data processing services should cover services that allow ubiquitous and on-demand network access to a configurable, scalable and elastic shared pool of distributed* ***computing resources****."* [complete quote on the next slide]
- Data Act, recital (85): "Switching is a customer-driven operation consisting of **several steps**, including **data extraction**, which refers to the downloading of data from the ecosystem of the source provider of data processing services; **transformation**, where the data is structured in a way that does not match the schema of the target location; and the **uploading** of the data in a new destination location."

More clarity about the interplay between the blockchain/DLT applications in the area of supply chain monitoring/management and the obligations for data processing services in the Data Act would be welcome.

9.6. Relevance of the DGA and the DSA?

Depending on the characteristics of the Blockchain/DLT use case the provisions of the Data Governance Act (DGA) and the Digital Services Act could be relevant, in particular if the use case qualifies as Data Intermediation Service or Data Altruism Organisation in the sense of the DGA or as Intermediary Service in the sense of the DSA. Reference is made to Chapter 11 below.

[150] Reference is made to Article 1(7) and recitals (80) and (85) of the Data Act. The switching and interoperability obligations for data processing services in Chapters VI and VIII of the Data Act apply services that qualify as services under Article 2(8) of the Data Act, meaning digital services with a focus on cloud service providers giving access to computing resources.


Deeper dive into the interplay between blockchain/DLT applications in the area of supply chain monitoring/management and the obligations for data processing services in the Data Act.
Interplay with the UN Transparency Protocol and Recommendation 49 also in light of the developments in the context of the UNECE consultation
Deeper dives into standardization in the context of the European Trusted Data Framework in combination with other relevant standardization initiatives.
Future discussions

10. Blockchain/DLT solutions for Battery Passports and DPP's and the interplay with horizontal Data Regulation

10.1. Introduction

The Battery Regulation and the ESPR (DPP's) was again one of the key regulatory areas for Blockchain/DLT solutions in the 2nd round of dialogues for the European Blockchain Sandbox.

Reference is made to Chapter 7 of the 1st cohort best practices report. In this section some parts of this report that served as a basis for the 2nd round of dialogues are quoted below in *blue*.

Report[151]:

- *On 17 August 2023, the new European Battery Regulation (EU 2023/1542)[152] entered into force. The regulation is part of the European Green Deal, which aims for the EU to become climate neutral by 2050. It establishes strict requirements regarding sustainability, performance, safety, labelling and information, collection and recycling of batteries. The regulation thereby governs the entire life cycle of batteries placed on the market in the EU, with the aim of strengthening a climate-friendly circular economy. Design and manufacturing of batteries should be geared towards optimising their performance, durability and safety and reducing their carbon footprint. In addition, the regulation aims to ensure that environmental and human rights due diligence requirements are complied with in the battery value chains.*

- *The Battery Regulation introduces a mandatory digital battery passport. From 18 February 2027 each light means of transport (LMT) battery, each industrial battery with a capacity greater than 2 kWh and each electric vehicle battery placed on the market or put into service shall have an electronic record ('battery passport').*[153]

- *On 27 May 2024, the Council of the EU approved the Ecodesign for Sustainable Products Regulation (ESPR)*[154] *which was the subject of an interinstitutional agreement on 5 December 2023 and had already been approved by the European Parliament on 23 April 2024. The ESPR is a framework regulation. Secondary legislation will determine the product groups and also the relevant levels (product, batch, category) for which the DPP requirement will become relevant including the applicable rules and requirements to be followed by DPP service providers. The EC will aim to conduct dialogues, consultations and studies with different stakeholders to identify best solutions in this regard. In determining the groups of products for which the DPP requirement will become relevant, the policy objectives of the DPP to simplify digital access to relevant product-specific information in the area of sustainability, circularity*

[151] Quotation from chapter 7, Battery Passports and DPP's, of the 1st cohort best practices report.
[152] The Regulation can be accessed in full through the following hyperlink: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1542.
[153] Article 77(1) Battery Regulation.
[154] Proposal for a Regulation of the European Parliament and of the Council establishing a framework for setting ecodesign requirements for sustainable products (COM/2022/142 final) and final approval to the ESPR by the European Council (https://www.consilium.europa.eu/en/press/press-releases/2024/05/27/green-transition-council-gives-its-final-approval-to-the-ecodesign-regulation/). The final Council text (Regulation of the European Parliament and of the Council of 16 May 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC (PE-CONS 106/23)) is available through: https://data.consilium.europa.eu/doc/document/PE-106-2023-INIT/en/pdf.

and legal compliance will be taken into account. In particular, durability and recyclability aspects will be carefully considered. The track and tracing functionality may also be included in the secondary legislation when appropriate. The product groups will be determined in the ESPR working plan that is expected withing 9 months after the entry into force of the ESPR and therefore during the first half of 2025. The industry, as well as national administrations, will have 18 months, after the adoption of the relevant delegated acts, to adapt to the new the eco-design requirements. However, in some duly justified cases, the Commission can set an earlier date of application.

10.2. Blockchain/DLT solutions for Battery Passports and DPPs under the Battery Regulation and the ESPR

Report[155]:

- *The Battery Regulation and the ESPR are based on the principle of technology neutrality. Further clarification and guidance to reflect this principle will be given through the standards and secondary legislation regarding compliance with the Battery Regulation and ESPR requirements in relation to DLT applications.*

- *The degree of information required on DPPs (static or dynamic) will depend on the product group and will be further defined in secondary legislation. An important point that will further be considered is the usefulness of dynamic information required on DPPs for the purpose of circularity. According to the Battery Regulation, certain categories of dynamic information will have to be part of the battery passports (Articles 14(1) and 45(2) and Annex VII).*

- *Blockchain solutions can be helpful to comply with due diligence obligations as laid down in Chapter VII of the Battery Regulation. The ESPR does not include due diligence provisions.*

- *Regulatory requirements in the Battery Regulation and the ESPR leave room for additional content/functionality as long as minimum requirements are met. The Battery regulation and ESPR do not include restrictions regarding the recording of additional/non-mandatory information, the use of such information and access rights.*

- *Compliance with other regulatory instruments like the GDPR, the AI Act, the Data Act, the Data Governance Act and NIS2 is relevant for the recording of data in Battery passports/DPPs and the use of and access rights to such data (mandatory and additional). These other regulatory instruments can also be particularly relevant if other technologies such as AI and IoT data analyses are used to monitor/verify the correctness of the data that is recorded on the blockchain.*

10.3. Status Update on Implementing Acts, Standards, and Interoperability Provisions for Battery Passports/DPPs since the 1st best practices report

Standardisation and the development of secondary legislation at EU level continue to play a crucial role for developing Battery Passports and DPP solutions. An overview of the status, implementation activities and timeline for the ESPR and DPP's can be found here: Ecodesign for Sustainable Products Regulation - European Commission.

With regard to standards, standards for DPP's including Battery Passports at EU level are currently being developed. As already mentioned in the European Blockchain Sandbox - Best

[155] Quotation from chapter 7, Battery Passports and DPP's, of the 1st cohort best practices report.

practices report. 1st Cohort, Part B - (**Chapter 7** – Battery Passports and DPP's), the European Commission has presented a standardisation request to the European Standardisation organisations (CEN/CENELEC, ETSI and national standardization bodies) for the implementation of DPP systems which was accepted by the standardization organisations. This request has now been published in the European Commission's online database of standardisation requests as Commission Implementing Decision C(2024) 5423.[156] In particular, standards have to be adopted by the end of 2025 in the following eight areas to support the implementation of the proposed DPP-system:

a) Unique identifiers,
b) Data carriers and links between physical product and digital representation,
c) Access rights management, information security, and business confidentiality,
d) Interoperability (technical, semantic, organisation)
e) Data processing, data exchange protocols, and data formats
f) Data storage, archiving, and data persistence,
g) Data authentication, reliability, integrity,
h) APIs for the DPP lifecycle management and searchability.

Specific requirements for each of these standards are laid down in Annex II to the Implementing decision.

Considering secondary legislation, as a first step[157], the European Commission will define additional technical specifications on DPPs in an upcoming Delegated Act laying down rules on the operation of DPP service providers.[158] From 18 February 2027, DPPs will become mandatory for certain types of batteries. To prepare for this first product group, the Commission is working on a delegated act setting out the requirements for DPP service providers.[159] The Commission has launched on 12 November a call for evidence for an impact assessment for the development of this delegated act, which is expected to be adopted by the second quarter of 2026.[160]

The delegated act will set out a framework for DPP services, a new niche digital industry market created by the ESPR. DPP service providers will be an important part of the DPP system, and it is essential for the new framework to create a fair and competitive market. In setting out this framework, the Commission aims to ensure support for responsible economic operators in complying with the ESPR requirements.[161] The requirements for DPP service

[156] Commission Implementation Decision of 31 July 2024 on a standardisation request to the European Committee for Standardisation, the European Committee for Electrotechnical Standardisation, and the European Telecommunications Standards Institute as regards digital product passports in support of Union policy on ecodesign requirements for sustainable products and on batteries and waste batteries.

[157] Article 11 of the ESPR empowers the Commission to adopt several pieces of secondary legislation related to the DPP. This call for evidence concerns the planned impact assessment for the first delegated act in that series, namely the delegated act 'setting out the requirements that digital product passport service providers are to comply with in order to become such providers, and, where appropriate, a certification scheme to verify compliance with such requirements'.

[158] According to Article 2(32) of the ESPR, this is a 'natural or legal person that is an independent third-party authorised by the economic operator which places the product on the market or puts it into service and that processes the digital product passport data for that product for the purpose of making such data available to economic operators and other relevant actors with a right to access those data under this Regulation or other Union law'.

[159] Article 11 of the ESPR empowers the Commission to adopt several pieces of secondary legislation related to the DPP. This call for evidence concerns the planned impact assessment for the first delegated act in that series, namely the delegated act 'setting out the requirements that digital product passport service providers are to comply with in order to become such providers, and, where appropriate, a certification scheme to verify compliance with such requirements'.

[160] The link with feedback received from stakeholders can be found here: Digital product passport – rules for service providers

[161] Besides, there is also the obligation to store a backup at the DPP service providers: Article 78(e) Battery Regulation, Article 9(2)(i) ESPR, Article 10(4) ESPR.

providers should not place a disproportionate burden on companies that would like to operate in this space and on other companies impacted by them.

In particular, the delegated act will set out requirements for DPP service providers, complementing those set out by the ongoing standardisation process. The possible requirements have been preliminarily grouped in three areas:

a) information security and (information) services of DPP data that responsible economic operators entrust to DPP service providers;
b) the financial viability of the DPP service providers to guarantee long-term access to DPP information;
c) assurance for businesses that DPP service providers comply with the requirements.

The Commission is planning to hold another public consultation on the draft text of the Delegated Act. Stakeholders will have the possibility to comment on the draft text of the Delegated Act and share their views with the Commission. The "Have your say" link can be found here: Digital product passport – rules for service providers. On the basis of the comments received from stakeholders to the upcoming public consultation, the Commission is planning to finalise the Delegated Act in the second half of 2025, for its adoption during the fourth quarter of 2025.

10.4. Data Deletion Requests / Continuity

During the dialogues the question was raised on how to handle requests to delete data from a specific supply chain actor in a DPP/Battery Passport when such data remains useful for the DPP/Battery Passport or the Economic Operator. Moreover, from an ESPR/Battery Regulation point of view, the economic operator has the liability for the availability of data under the DPP.

If an Economic Operator hosts a DPP themselves, there needs to be a backup for the persistency of information for some years with a digital product passport service provider.[162] Contractual arrangements between the Economic Operator and the supply chain operators to make sure that the information remains available in accordance with the applicable regulatory requirements – and therefore deletion of such data from the DPP cannot be requested by supply chain actors as this would be inconsistent with the obligations of the Economic Operator - are recommended.

10.5. Interplay between the Battery Regulation/ESPR and the Data Act

As mentioned in the previous chapter, the horizontal data regulation instruments and the sector- and domain-specific initiatives focused on data sharing are part of the European single market for data.

Depending on the characteristics of the DLT use case the provisions regarding data sharing/access, switching between (data) processing services and interoperability in sectoral and domain-specific EU legislation such as the ESPR and the Battery Regulation and in horizontal EU data regulatory instruments such as the Data Act, the Data Governance Act and the Digital Services Act may apply in parallel.

10.5.1. Battery Regulation/ESPR

The Battery Regulation and the ESPR require that information included in battery Passports/DPP's shall be based on open standards and shall be interoperable with other

[162] Article 78(e) Battery Regulation, Article 9(2)(i) ESPR, Article 10(4) ESPR.

passports that are required under EU law.[163] The Battery Regulation/ESPR do not provide specific obligations to facilitate switching between DPP/Battery Passport solutions but this will likely become part of the Delegated Act for service providers.

The standardization in the eight areas listed in the Commission Implementing Decision C(2024) 5423 of 31 July 2024[164] will ensure interoperability and support switching between and parallel use of DPP/Battery Passport solutions in accordance with the specific requirements for the standards in the area of *"interoperability (technical, semantic, organization)"* and in the area of *"data processing, data exchange protocols, and data formats"* laid down in Annex II to the Implementing decision:

- Interoperability (technical, semantic, organisation)
  - *The standard(s) shall define, inter alia, rules related to the following: (a) semantic description of a product, including but not limited to unambiguous meaning and consistent naming and, where relevant, a value list, a specific format and defined units of measure for all quantitative values; (b) a common information model allowing for the implementation of dictionary systems; (c) metadata models and formats to be used in exchange and representation. The standard(s) shall include rules on how to systematically use such metadata models when developing product group specific data models*
- Data processing, data exchange protocols, and data formats
  - *These standard(s) shall define, inter alia, rules related to the following: (a) data exchange protocols, including rules to exchange data between two or more parties; (b) processes to introduce, modify, and update information in the product passport*

With regard to data sharing obligations, the ESPR aims to prevent that DPP service providers use data from companies without companies' consent. A provision was therefore added in the Battery Regulation (Article 78), the ESPR (Article 11) and in the Commission Implementing Decision C(2024) 5423 to prevent this to happen. However, a company can agree to the sale, re-use or processing of its own data in a Digital Product Passport for other purposes.

10.5.2. Data Act

The Data Act lays down obligations for data processing services and interoperability. Chapter VI of the Data Act[165] contains obligations for providers of data processing services to facilitate switching between data processing services. Chapter VIII of the Data Act[166] lays down obligations to ensure interoperability between participants in "data spaces" as well as obligations to ensure in-parallel use of data processing services and interoperability of data processing services.

The terms "data processing service", "switching" and "interoperability" are defined in the Data Act.[167]

Whether the obligations regarding switching between data processing services and interoperability in the Data Act are applicable to Blockchain/DLT solutions for Battery Passports/DPPs will depend on the characteristics of the use case. The provisions of Chapter VI Data Act (switching between data processing services) will likely not apply to

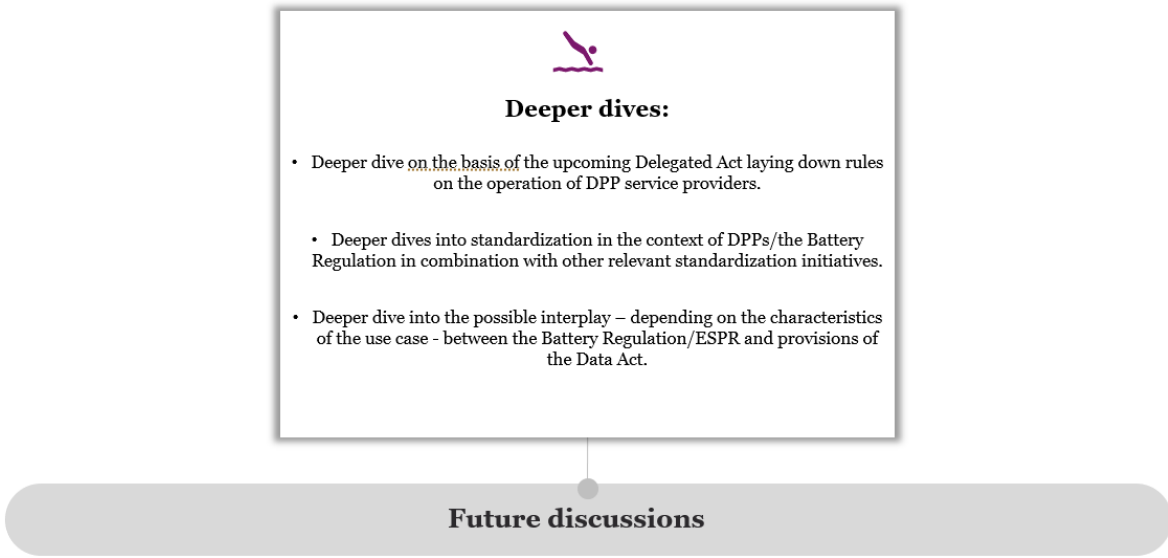
[163] Articles 77(5) and 78(a) Battery Regulation; Articles 10(1)(d) and 11 ESPR.
[164] See paragraph 2 above.
[165] Articles 23 – 31 Data Act.
[166] Articles 33 – 36 Data Act.
[167] Article 2(8), 2(34) and 2(40) Data Act. See definitions in previous chapter.

blockchain/DLT use cases that act as a data intermediary merely using digital services/cloud services and not providing such services.[168] However, as mentioned above, switching between DPP/Battery Passport solutions will likely become part of the Delegated Act for service providers on the basis of the ESPR.

Although it is not 100% clear if a DPP should/needs to be considered a data space in the sense of Article 33 of the Data Act or not, there seems to be no direct impact as the data sharing and requirements from the DPP (ESPR/battery regulation) should be in line with the Data Act and could probably also be considered "lex specialis".[169] A confirmation about this possible interplay between the Battery Regulation/ESPR and the aforementioned provisions of the Data Act would be welcome.

10.6. Relevance of the DGA and the DSA?

Depending on the characteristics of the Blockchain/DLT use case the provisions of the Data Governance Act (DGA) and the Digital Services Act could be relevant, in particular if the use case qualifies as Data Intermediation Service or Data Altruism Organisation in the sense of the DGA or as Intermediary Service in the sense of the DSA. Reference is made to Chapter 11 below.



[168] Reference is made to Article 1(7) and recitals (80) and (85) of the Data Act. The switching and interoperability obligations for data processing services in Chapters VI and VIII of the Data Act apply services that qualify as services under Article 2(8) of the Data Act, meaning digital services with a focus on cloud service providers giving access to computing resources.

[169] Blockchain/DLT solutions for Battery Passports/DPPs will have to comply with the standards that will be adopted by the end of 2025 in accordance with the Commission implementing decision of 31 July 2024 referred to in paragraph I. If DPPs/Battery Passports would qualify as "data spaces" in the sense of Article 33(1) Data Act, DPPs/Battery Passports that meet the harmonised standards[169] shall be presumed to be in conformity with the essential requirements in the area of interoperability: reference is made to Article 33(8) Data Act.

11. Compliance with the Data Governance Act and the Digital Service Act

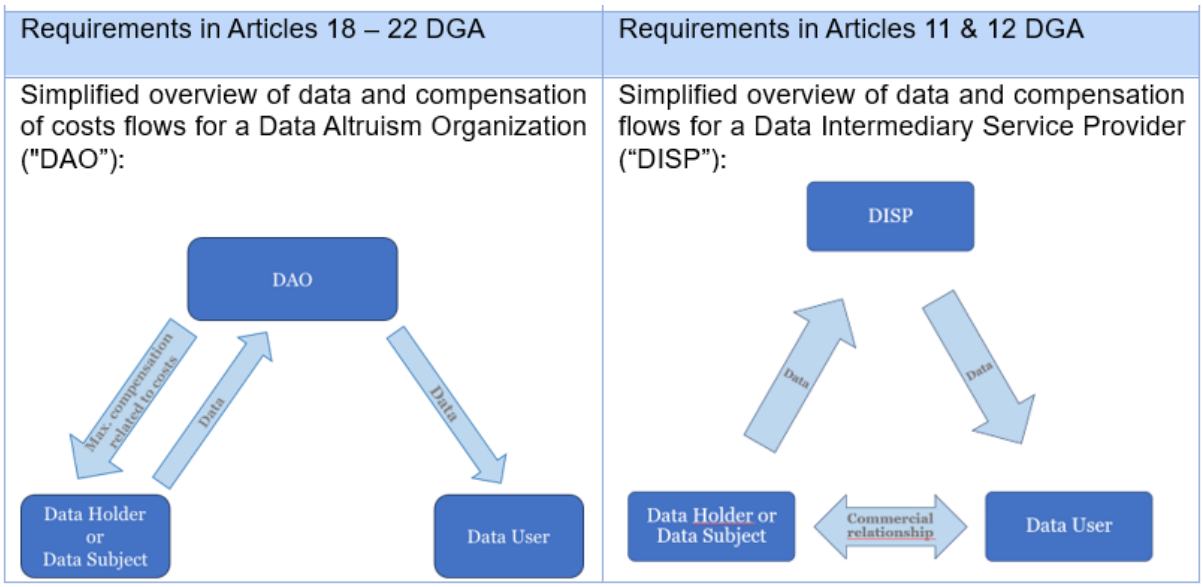
11.1. Applicability of the DGA to Blockchain/DLT solutions?

The DGA could be a relevant regulatory area for Blockchain/DLT solutions depending on the characteristics of the use case. The DGA was discussed as part of the 1st round of dialogues with a focus on Data Altruism Organisations.

Reference is made to Chapter 10 of the 1st cohort best practices report. In this section some parts of this report that served as a basis for the 2nd round of dialogues are quoted below in *blue*.

Report[170]:

- *In view of the fact that the DGA is relatively new and uses novel legal concepts, the most efficient way forward will normally be that the use case owner discusses the qualification of the service with the competent authority/authorities to determine which regulatory obligations apply and if notification/registration is mandatory/feasible.*



Data Intermediation Services are defined in Article 2(11) of the Data Governance Act.

Article 2(11) Data Governance Act – definition of Data Intermediation Service

(11) 'data intermediation service' means a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, excluding at least the following:

170 Quotation from chapter 10, Data Governance Act, of the 1st cohort best practices report.

(a) services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users;

(b) services that focus on the intermediation of copyright-protected content;

(c) services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group, including supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things;

(d) data sharing services offered by public sector bodies that do not aim to establish commercial relationships;

Article 10(a) Data Governance Act – Data intermediation services subject to DGA regulatory requirements

The provision of the following data intermediation services shall comply with Article 12 and shall be subject to a notification procedure:

(a) intermediation services between data holders and potential data users, including making available the technical or other means to enable such services; those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint use of data, as well as the establishment of other specific infrastructure for the interconnection of data holders with data users;

(b) intermediation services between data subjects that seek to make their personal data available or natural persons that seek to make non-personal data available, and potential data users, including making available the technical or other means to enable such services, and in particular enabling the exercise of the data subjects' rights provided in Regulation (EU) 2016/679;

(c) services of data cooperatives.[171]

Data Intermediation Services between data holders and potential data users, *including making available the technical or other means to enable such services* are subject to a notification procedure to the relevant national competent authority for data intermediation services in accordance with Articles 10 and 11 of the DGA and have to comply with the regulatory requirements of Article 12 DGA.[172] The notification process is simple and will allow the provider to declare itself a trusted intermediation service.

[171] Article 2(15) DGA - 'services of data cooperatives' means data intermediation services offered by an organisational structure constituted by data subjects, one-person undertakings or SMEs who are members of that structure, having as its main objectives to support its members in the exercise of their rights with respect to certain data, including with regard to making informed choices before they consent to data processing, to exchange views on data processing purposes and conditions that would best represent the interests of its members in relation to their data, and to negotiate terms and conditions for data processing on behalf of its members before giving permission to the processing of non-personal data or before they consent to the processing of personal data;

[172] The requirements for Data Intermediation Services do not apply to recognized data altruism organisations and certain other not-for-profit entities as specified in Article 15 DGA.

- The EU register of data intermediation services can be found here: EU register of data intermediation services | Shaping Europe's digital future

Data intermediation services are considered particularly important in the context of the establishment of common European Data Spaces, namely purpose- or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data for, inter alia, the development of new products and services, scientific research or civil society initiatives:[173]

> *"(28) Examples of data intermediation services include data marketplaces on which undertakings could make data available to others, orchestrators of data sharing ecosystems that are open to all interested parties, for instance in the context of common European data spaces, as well as data pools established jointly by several legal or natural persons with the intention to license the use of such data pools to all interested parties in a manner that all participants that contribute to the data pools would receive a reward for their contribution."*

Blockchain/DLT applications will likely only qualify as a Data Intermediation Service if they aim to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other. Therefore, a service on behalf of a specific economic operator to provide specific information to different categories of stakeholders (general public, authorities and persons with a legitimate interest) will likely not qualify as a data intermediation service in the sense of the DGA.

However, this could be different if the DLT/blockchain solution can be used by any operator/trader/data holder and an undetermined group of data users in the Green Deal Data Space.

More clarity about the question if/under what conditions Blockchain/DLT applications that support compliance with ESG regulation regarding data collection, reporting and data access establish "commercial relationships" in the sense of Article 2(11) of the Data Governance Act would be welcome.

11.2. Applicability of the DSA – Qualification of Blockchain/DLT solutions as "intermediary service"

Intermediary services are defined in Article 3(g) of the Digital Services Act.

Article 3(g) Digital Services Act – definition of" Intermediary service"

3(g) 'intermediary service' means one of the following information society services:

(i) a 'mere conduit' service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;

(ii) a 'caching' service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;

[173] Recital (28) DGA.

> *(iii) a 'hosting' service, consisting of the storage of information provided by, and at the request of, a recipient of the service;*

Online platforms are hosting services with certain characteristics set out in Article 3(i) of the DSA:

Article 3(i) Digital Services Act – definition of "online platform"

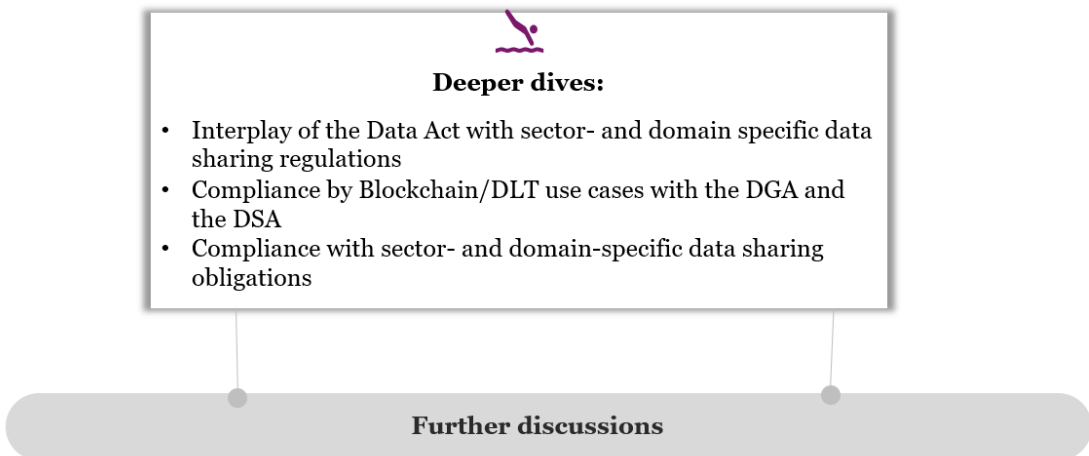
> *3(i) 'online platform' means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation;*

It appears unlikely that a DLT/Blockchain use case qualifies as a hosting service if only a link is stored on-chain by the use case, which is used to verify off-chain information stored by the customer.

However, more clarity on when a DLT/Blockchain use case qualifies as a hosting service would be beneficial.

11.3. Areas for further clarification & dialogue topics for the next cohorts

Chapters 9, 10 and 11 cover the broad area of the European Single Market for Data. If and to what extent individual data sharing regulatory instruments are applicable to Blockchain/DLT solutions and the interplay between the different regulations (Data Act, DGA and DSA as well as sector- and domain specific) will likely be an important area for the 3rd round of dialogues.



12. Blockchain/DLT solutions to enhance compliance with sanctions lists

12.1. Introduction

EU entities and persons should comply with EU sanctions lists and (where applicable) relevant national sanctions lists.

The legal framework for EU sanctions can be found in various EU regulations. In the so-called 'Consolidated Financial Sanctions List', persons, groups and entities who are subject to EU financial sanctions can be found.[174]

- EU entities should in the first place observe EU sanctions lists and national sanctions lists. Sanctions lists from other jurisdictions should be observed if there is a particular justification to that e.g. that entity conducts business in that other jurisdiction or is a subsidiary of a company from that other jurisdiction.

References to EU sanctions can be found in various pieces of legislation, including the AML legislation. According to Annex III of ALMD5[175], countries that are (inter alia) subject to sanctions issued by, for example, the EU or the UN are considered as a 'geographical risk factor'. The latter implies that EU Members states and obliged entities must take this factor into account when assessing the risk of money laundering and terrorist financing. In other words, ALMD5 refers to sanctions only as a geographical risk factor as part of the CDD.

By contrast, the AMLR[176] is more comprehensive in its refence to sanctions. For example, the AMLR not only deals with various definitions of (targeted) financial sanctions but also provides for CDD measures to mitigate any risk of non-implementation or evasion of targeted financial sanctions – such as verifying whether parties are, directly or indirectly, subject to targeted financial sanctions. In this regard, the AMLR requires that obliged entities must at all times be able to demonstrate to their supervisors that the latter measures taken are appropriate in view of the identified money laundering and terrorist financing risks.

12.2. Best practices and lessons learned

Blockchain/DLT solutions that support (almost) real time implementation of compliance with sanctions lists in a consistent and immutable/auditable manner across branches and group companies can enhance efficiency and effectiveness of compliance with sanctions regulations.

Such solutions could also have benefits for regulators/authorities and obliged entities and do appear to enhance effective and efficient oversight for regulators as regulators could follow a timestamped and solid audit trail which is the same among branches and across jurisdictions. This could also make the collaboration between different regulators and between regulators and obliged entities more efficient.

[174] https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en.
[175] Directive (EU) 2015/849.
[176] Regulation (EU) 2024/1624.

Blockchain/DLT solutions can enhance effective and efficient compliance and oversight of sanctions lists

- Blockchain/DLT solutions that support (almost) real time implementation of compliance with sanctions lists in a consistent and immutable/auditable manner across branches and group companies can enhance efficiency and effectiveness of compliance with sanctions regulations.
- Such solutions could also have benefits for regulators/authorities and obliged entities and do appear to enhance effective and efficient oversight for regulators as regulators could follow a timestamped and solid audit trail which is the same among branches and across jurisdictions.
- This could also make the collaboration between different regulators and between regulators and obliged entities more efficient.

13. Blockchain/DLT solutions to enhance AML compliance

13.1. Introduction

The AML regulatory framework consists of the AML Directive[177] and the national implementations thereof, the AMLR[178] and the TFR.[179]

Compliance with AML requirements can be a relevant area for many Blockchain/DLT use cases for various reasons. On the one hand Blockchain/DLT applications could qualify as "obliged entities" in the sense of the AML regulatory framework and on the other hand Blockchain/DLT applications that can support AML compliance by other "obliged entities".

AML requirements were one of the key regulatory areas in the 1st round of dialogues and were again an important area in the 2nd round.

Reference is made to Chapter 12 of the 1st cohort best practices report. In this section some parts of this report that served as a basis for the 2nd round of dialogues are quoted below in *blue*.

Report:[180]

- *The obligations laid down in the AMLD IV include risk assessment, identification and verification of the identity of clients and their beneficial owners, due diligence measures upon entry and throughout the business relation, obligation to file suspicious transaction reports to Financial Intelligence Units (FIUs), internal audit and reporting, and implementation of asset freezing measures.*

- *The AMLD V sets out a series of measures aimed at combating terrorist financing more effectively and guaranteeing more transparency in financial transactions. This directive aims to make legal entities and legal structures more transparent by extending access to beneficial owner registers, harmonizing the enhanced due diligence measures to be implemented for business relationships or transactions that involve high-risk third countries, specify the measures to be implemented in the event of a creation of a remote business relationship, and provide for certain virtual asset service providers to be regulated under the anti-money laundering and countering the financing of terrorism (AML/CFT) rules.*

- *Additionally, the Transfer of Funds Regulation[181] will apply also to CASPs. CAPSs will be obliged to collect and make accessible certain information about the sender and beneficiary of the transfers of crypto assets they operate, regardless of the amount of crypto assets being transacted. This ensures the traceability of crypto-asset transfers in order to be able to better identify possible suspicious transactions and, as necessary, block them. To this end, the EBA has issued amended guidelines on CDD requirements for risks associated with crypto asset service providers.[182]*

---

177 The consolidated version of the AMLD IV/V/VI is published here: CL2015L0849EN0010010.0001.3bi cp 1..1

178 Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financingText with EEA relevance.

179 Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1113.

180 Chapter 12, Blockchain solutions and AML compliance, 1st cohort best practices report (June 2024).

181 Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849.

182 Available via: https://www.eba.europa.eu/sites/default/files/2024-01/a3e89f4f-fbf3-4bd6-9e07-35f3243555b3/Final%20Amending%20%20Guidelines%20on%20MLTF%20Risk%20Factors.pdf.

- *Lately, a new AMLD VI was proposed by the European Commission in July 2021 and has been adopted by the European Parliament on 24 April 2024 and is currently awaiting the Council's 1st reading.*[183] *In order to effectively detect criminals attempting to misuse the financial systems for illegal purposes and to further strengthen the integrity of the internal market, further improvement of the current framework was considered necessary by the European Commission. The AMLD VI will, for example, lead to changes in the field of ultimate beneficial owners and the powers of FIUs in relation to pending transactions.*

- *Alongside the adoption of the AMLD VI on 24 April, the European Parliament also adopted the 'EU Single Rulebook Regulation', the so-called "**AMLR**".*[184] *This new legislative measure mainly covers the gap due to the lack of directly applicable rules under the current AML directives. This new harmonized approach should enable a strong and coherent approach at Union level to prevent money laundering and predicate offences. In the AMLR currently includes a list of obliged entities applicable in all EU Member, exemptions for certain activities and companies, facilitating compliance for cross-border obligations and additional requirements for internal policies, procedures and controls.*

The EU AML legislation was amended in 2024 when the following legal instruments were adopted:

- Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 (**"AMLD 6"**) must be transposed in national legislation by 10 July 2027.[185]
- Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 ("**AMLR**") will also become applicable on 10 July 2027.[186]
- Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism ("**AMLA-R**"). will mostly start to apply as of 1 July 2025.

In addition, the Transfer of Funds Regulation (EU) 2023/1113 (**TFR)** became applicable as of 30 December 2024.

The aim of the amended AML legislation is in particular to i) improve the ability of the financial system to detect suspicious transactions and activities, closing gaps exploited by criminals to launder illicit proceeds or finance terrorist activities and ii) adapt the current regulatory framework of the Union to new and emerging challenges related to technological innovation, the increased integration of financial flows in the single market and the global nature of terrorist organizations.

---

[183] *The status and consolidated* text so far are accessible via: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0250(COD)&l=en.

[184] The status and consolidated text so far are accessible via: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0239(COD)&l=en.

[185] AMLD4, as amended by the AMLD 5 will be repealed on that date. Certain amendments in relation to the accessibility of central registers of beneficial ownership of corporates and trusts will have to be implemented earlier: UBO registers - Article 74 AMLD 6), must be transposed by 10 July 2025 and Article 11-13 and 15 AMLD 6, also addressing beneficial owner registers, have to be transposed by 10 July 2026. Provisions regarding the single access point to real estate information (Article 18 AMLD 6) will have to be transposed later (by 10 July 2029).

[186] Except for the provisions which bring football agents and professional football clubs (in relation to certain types of transactions) into the scope of obliged entities, which will start to apply from 10 July 2029.

AML is another important regulatory area for blockchain/DLT applications from different perspectives:

- A broad range of legal and natural persons qualifying as obliged entities in the sense of the AMLD[187] and the AMLR[188] have to comply with AML requirements. This includes entities qualifying as virtual asset service providers under financial sector regulation and CASPs under MiCAR.
- Blockchain/DLT providers provide tools to support obliged entities to ensure AML compliance in their business relationships with crypto exposure.

If a token is neither covered by MiCAR nor by MiFID, AML regulation will still be relevant for obliged entities dealing with such tokens and the obliged entity will still need to include this in its general risk assessment.[189]

In addition to the 1st round of regulatory dialogues[190], the 2nd round of AML/CDD dialogues focused on:

- Relevant regulations in the area of outsourcing/third party service providers – The interplay with DORA.[191]
- The interplay with the GDPR.[192]
- The interplay of the AML/CDD obligations and the eIDAS regulation.[193]

13.2. Outsourcing/third party service provision of AML regulatory requirements

The possibilities for obliged entities to rely on the customer information collected by other obliged entities is currently not harmonized[194], but this will change under the AMLR which provides for harmonized provisions regarding the reliance on information collected by other obliged entities in Articles 48 – 50 AMLR. By 10 July 2027, AMLA shall issue guidelines regarding reliance on other obliged entities.

Report:[195]

- *Different criteria impacting the assessment of whether a procured service qualifies as outsourcing*[196]*, as well as coexistence of various outsourcing regimes (i.e, AML outsourcing*[197]*, sector-specific outsourcing regimes applicable to financial*

[187] Directive EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (link).
[188] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Text with EEA relevance) (link).
[189] Apart from the AML regulation also possible consequences under criminal law and in the national law of the Member States may be relevant.
[190] Best practices report, 1st cohort, chapter 12.
[191] See chapter 14 DORA.
[192] See chapter 3 GDPR.
[193] See chapter 4 eIDAS.
[194] Reference is made to for instance the national laws in Germany, France and Iceland providing national law provisions allowing re-use of information collected by other obliged entities under certain conditions. In Spain, entities within the same category, as defined in Article 2 of the Spanish Law 10/2010, of April 28, on the prevention of money laundering and the financing of terrorism, can create common systems for information, storage, and access to comply with due diligence obligations, except for continuous monitoring of business relationships regulated in Article 6. The AML authority may authorize the establishment of common systems in which various categories of obligated entities participate, defining these categories and the information that may be shared.
[195] Quotations from Chapter 12, Blockchain/DLT solutions for AML Compliance, 1st cohort best practices report (June 2024).
[196] Par. 26 and 27 EBA Outsourcing Guidelines.
[197] Section 4 of Directive (EU) 2015/849.

institutions[198], EBA and ESMA guidelines on outsourcing[199]) may lead to uncertainty for service providers and financial institutions if services they provide / receive qualify as regulated outsourcing. This is another area were more guidance would be welcome.

- *If a financial entity purchases a license for standardised software that does not entail data exchange between the entity and the software provider, such an arrangement should not be considered outsourcing. However, as mentioned above, it is important to note that the application of DORA will introduce an ICT third-party risk management framework that extends beyond outsourcing ICT agreements, encompassing any contractual arrangements with an ICT third-party service provider.*

The overview below could be helpful to analyse rights and obligations in outsourcing/third party service provision regulatory obligations:

	AMLD IV/V	**AMLR**	**DORA**	**EBA Guidelines**
Scope of regulated outsourcing / third-party provision	CDD, but not continuous monitoring (Art. 25)	Tasks resulting from the AMLR (Art. 18)	ICT services (Art. 3(21))	Outsourcing (par. 5)
Ultimate responsibility	Obliged entity (Art. 25)	Obliged entity (Art. 18(2))	Obliged entity (Art. 28(1)(a))	Management bodies of credit institutions, investment firms, payment institutions and electronic money institutions (par. 35)
Prior notification or approval?	Dependent on national implementation (Art. 25)	Prior notification required (Art. 18(1))	Prior notification and annual reporting required (Art. 28(3))	Information or dialogue with the competent authority about planned outsourcing of critical or important functions (par. 58)

198 E.g., Article 19(6) of Directive (EU) 2015/2366 (PSD2) or Article 73 of Regulation (EU) 2023/1114 (MiCAR)

199 EBA Guidelines on outsourcing arrangements - 25 February 2019, EBA/GL/2019/02 (Accessible via: https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf), Paragraph 26: *"Institutions and payment institutions should establish whether an arrangement with a third party falls under the definition of outsourcing. Within this assessment, consideration should be given to whether the function (or a part thereof) that is outsourced to a service provider is performed on a recurrent or an ongoing basis by the service provider and whether this function (or part thereof) would normally fall within the scope of functions that would or could realistically be performed by institutions or payment institutions, even if the institution or payment institution has not performed this function in the past itself." See also ESMA, 'Guidelines - On outsourcing to cloud service providers' (10 May 2021, ESMA50-164-4285, via: https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines.pdf).*

Outsourcing/ contractual arrangement register	Dependent on national implementation (Art. 25)	Not specifically required	Yes (Art. 28(3))	Yes (par. 52-60)
Substantive requirements outsourcing / third-party supplier contract	Dependent on national implementation	By 10 July 2027, AMLA shall issue guidelines addressed to obliged entities (Art. 18(8))	Detailed in DORA: general principles (Art. 28), preliminary assessment of ICT concentration risk at entity level (Art. 29), key contractual provisions (Art. 30)	Includes detailed provisions re. outsourcing arrangements (Title II), governance frameworks surrounding outsourcing (Title III) and processes and measures in relation to outsourcing (Title IV)

13.3. Applicability of the Transfer of Funds Regulation to e-money tokens

E-money tokens are considered both as crypto-assets under MiCAR[200] and as e-money in accordance with the E-Money Directive. E-money tokens can therefore be qualified as funds through both legislative instruments and are consequentially in scope of the TFR.

Irrespective of e-money tokens being deemed as funds (Article 48(2) MiCAR), they are treated as crypto-assets for the purposes of the TFR (Article 2(4) TFR). Therefore, in case e-money tokens are used in the cash leg of a settlement system, Chapter 3 of the TFR is applicable.[201]

13.4. Areas for further clarification and dialogue

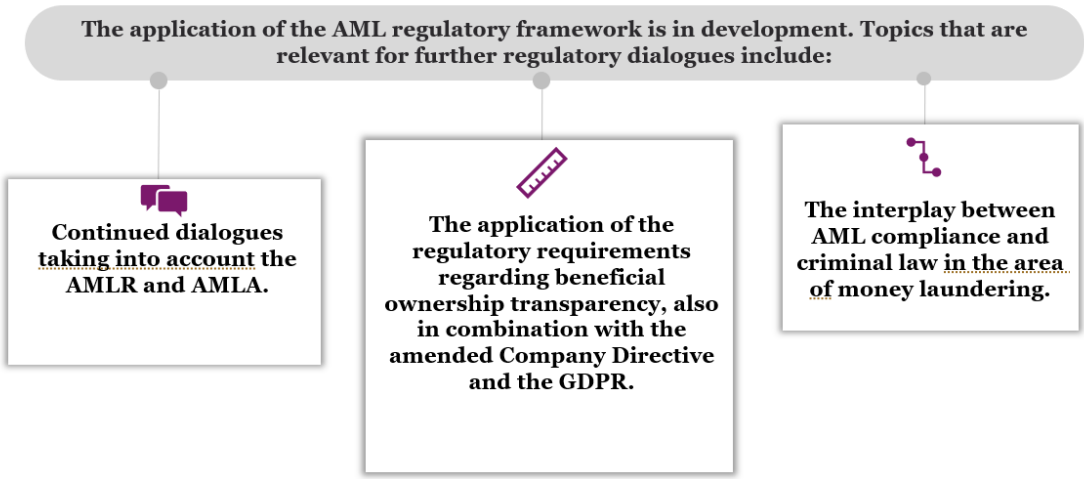
The application of the AML regulatory framework is in development. Topics that are relevant for further regulatory dialogues include:

- Continued dialogues taking into account the AMLR and AMLA.
- The application of the regulatory requirements regarding beneficial ownership transparency, also in combination with the amended Company Directive[202] and the GDPR.
- The interplay between AML compliance and criminal law in the area of money laundering.

[200] https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng; ESMA75-223375936-6099 Statement on the provision of certain crypto-asset services in relation to non-MiCA compliant ARTs and EMTs (europa.eu) and EBA statement on Application of MiCAR to ARTs and EMTs.pdf (europa.eu)

[201] In other parts of the settlement system, the TFR is not applicable to tokenised financial instruments due to definition of crypto-asset in TFR ('crypto-asset' means a crypto-asset as defined in Article 3(1), point (5), of MiCAR, except were falling within the categories listed in Article 2(2), (3) and (4) of MiCAR or otherwise qualifying as funds).

[202] See also chapter 4.3.


The application of the AML regulatory framework is in development. Topics that are relevant for further regulatory dialogues include:
Continued dialogues taking into account the AMLR and AMLA.
The application of the regulatory requirements regarding beneficial ownership transparency, also in combination with the amended Company Directive and the GDPR.
The interplay between AML compliance and criminal law in the area of money laundering.

14. DORA - Regulatory compliance

14.1. Introduction

DORA is an important piece of cybersecurity legislation that covers a wide range of regulated financial entities at EU level and their relations with ICT third-party service providers, in order to ensure that ICT-risks are managed in a homogeneous and consistent way.[203] As a regulation, DORA is directly applicable in all EU Member States from 17 January 2025.

DORA lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities and addresses both, the digital as well as physical dimension. It constitutes the *lex specialis* regarding the NIS2 Directive[204] and addresses in a comprehensive manner the physical resilience of financial entities with the consequence that certain provisions set out in the CER Directive[205] do not apply to those entities.

- The NIS2 Directive was one of the important relevant areas for Blockchain/DLT use cases in the 1st round of dialogues. Reference is made to Chapter 4 of the 1st cohort best practices report.

DORA regulatory requirements are laid down in the different chapters of the Regulation and the Delegated Regulations: ICT Risk Management[206], ICT-related incident management, classification & reporting[207], Digital operational resilience testing[208] and Managing of ICT third-party risk[209].
More detailed regulations on the basis of DORA provisions are laid down in Regulatory Technical Standards (RTS) as well as Implementing Technical Standards (ITS) which are of high relevance. An overview of the Implementing and delegated acts for DORA can be found here: Digital Operational Resilience Regulation - European Commission (europa.eu).

14.2. Key Question: To what extent are DORA regulatory requirements relevant for DLT/Blockchain solution providers?

For DLT/Blockchain solution providers DORA regulatory requirements could be of direct or indirect relevance.

14.2.1. Direct relevance of DORA for DLT/Blockchain providers which qualify as "financial entities"

The regulation does not explicitly mention DLT/blockchain providers as entities directly subject to DORA. However, the regulatory requirements laid down in DORA are directly applicable to DLT/blockchain solution providers which qualify as a "financial entity" in the sense Article 2(1)

[203] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, available here.
[204] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive), available here.
[205] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER Directive), available here.
[206] Chapter II DORA.
[207] Chapter III DORA.
[208] Chapter IV DORA.
[209] Chapter V DORA.

DORA.[210] Crypto-asset service providers authorised under MiCAR and issuers of asset-referenced tokens qualify as "financial entities" under DORA and are therefore subject to the various obligations it imposes.

Regulatory requirements of direct relevance for "financial entities" (or having indirect effect on their ICT third-party service providers) relate to:[211]

- ICT risk management – Chapter II, Articles 5 – 16 DORA;
- ICT-related incident management, classification and reporting – chapter III, Articles 17 – 23 DORA;
- Digital operational resilience testing – Chapter IV, Articles 24 – 27 DORA;
- Managing of ICT third-party risk, including requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities – Chapter V, Articles 28 – 30 DORA;

DORA provides for a lighter regulatory regime for microenterprises[212] and does not apply to certain financial entities that are subject to lighter requirements or exemptions for reasons associated with their size or the services they provide.[213]

On the other hand, DORA provides a specific regulatory regime for ICT third-party service providers which qualify as "critical ICT third-party service provider".[214] Critical ICT third-party service providers are critical for financial entities, taking into account, inter alia, their systemic impact on, character or importance to the financial services, as well as their substitutability and the extent to which critical or important functions of financial services rely on them.

14.2.2. Indirect relevance of DORA for DLT/Blockchain solution providers that qualify as "ICT third-party service provider"

DORA also applies (indirectly) to "ICT third-party service providers".[215] Chapter V, Section I, Articles 28 – 30 DORA lays down regulatory requirements for financial entities[216] regarding the management of their ICT third-party risks.[217]

Reference is made to the following definitions:

- Article 3(7) DORA: 'ICT asset' means a software or hardware asset in the network and information systems used by the financial entity;

---

[210] According to Article 2(2) DORA "financial entities" in the sense of DORA include (a) credit institutions; (b) payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366; (c) account information service providers; (d) electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC; (e) investment firms; (f) crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('the Regulation on markets in crypto-assets') and issuers of asset-referenced tokens; (g) central securities depositories; (h) central counterparties; (i) trading venues; (j) trade repositories; (k) managers of alternative investment funds; (l) management companies; (m) data reporting service providers; (n) insurance and reinsurance undertakings; (o) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries; (p) institutions for occupational retirement provision; (q) credit rating agencies; (r) administrators of critical benchmarks; (s) crowdfunding service providers; (t) securitisation repositories.

[211] Article 1(1) DORA.

[212] According to Article 3(60) DORA *'microenterprise' means a financial entity, other than a trading venue, a central counterparty, a trade repository or a central securities depository, which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed EUR 2 million*.

[213] Article 2(3) DORA. In addition, Article 16 provides for a Simplified ICT risk management framework for certain financial entities.

[214] Chapter V, Section II, Articles 31 – 44 DORA.

[215] See Art. 2(1) lit. u) DORA).

[216] "Financial entities" as defined in Article 2 DORA.

[217] Chapter V, Section I, Articles 28-30 DORA.

- Article 3(18) DORA: 'ICT third-party risk' means an ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements;

- Article 3(19) DORA: 'ICT third-party service provider' means an undertaking providing ICT services;

- Article 3(21) DORA: 'ICT services' means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services;

- Article 3(22) DORA: 'critical or important function' means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law;

Article 28 DORA sets out the general principles to which financial entities should comply regarding contractual arrangements, the adoption and regular review on strategy on ICT third-party risk and registration of information in relation to all contractual arrangements with ICT third-party providers. Article 30(2) DORA sets out the minimum elements to be included in contractual arrangements on the use of ICT services.

According to Article 28 – 30 DORA, additional requirements are applicable regarding contractual arrangements in relation to ICT services supporting critical or important functions such as:

- the obligation to inform the competent authority in a timely manner about any planned contractual arrangement on the use of ICT services supporting critical or important functions as well as when a function has become critical or important;[218]

- due diligence and risk assessment regarding the use of subcontractors supporting critical or important functions;[219]

- additional elements to be included in contractual arrangements on the use of ICT services supporting critical or important functions.[220]

The ESA's have developed draft regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers which have been adopted by the European Commission in accordance with Article 28(10) DORA: Link

[218] Article 28(3) DORA.
[219] Article 29 DORA.
[220] Article 30(2) DORA. According to Article 30(5) DORA, the ESAs shall develop draft regulatory technical standards to specify further the elements referred to in paragraph 2, point (a), which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions. The ESAs published a final report about this RTS on 26 July 2024 (available via this link: https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024_53_Final_report_DORA_RTS_on_subcontracting.pdf). On 21 January 2025, the EC responded in a letter it rejected this draft RTS as Article 5 and the related recital 5 exceeded the mandate given in Article 30(5) DORA (available via this link: https://finance.ec.europa.eu/document/download/9a7139d5-1cbf-4dca-a5cf-853467b375c7_en?filename=250124-letter-esas_en.pdf). The ESAs responded to the letter of the EC on 7 March 2025 (available via this link: https://www.esma.europa.eu/sites/default/files/2025-03/JC_2025_06_-_ESAs_Opinion_on_the_rejection_of_the_RTS_on_subcontracting_under_DORA.pdf).

Note: A distinction should be made between ICT third-party service providers supporting "critical or important functions" as defined in Article 3(22) DORA and "critical ICT third-party service provider" in the sense of Article 3(23) DORA, meaning an ICT third-party service provider designated as critical in accordance with Article 31 DORA and governed by Chapter V, Section II DORA.

14.3. Best practices and lessons learned

14.3.1. Qualification of Blockchain/DLT solutions as ICT third-party service providers - supporting critical or important functions?

Blockchain/DLT solutions will normally qualify as ICT assets in the sense of Article 3(7) DORA. Therefore, the DORA requirements for financial entities regarding their contractual arrangements with ICT third-party service providers laid down in Chapter V, Section I, DORA will normally be applicable in relation to the provision of Blockchain/DLT solutions (key principles for a good management of ICT third-party risks).

Certain Blockchain/DLT solutions can be deployed by "financial entities" to enhance compliance with relevant regulations such as sanctions regulation.

Compliance with sanctions regulation may qualify as a "critical or important function" as defined in Article 3(22) DORA, meaning that the additional DORA requirements for ICT third-party service providers supporting critical or important functions in Chapter V, Section I, DORA appear to be applicable as well.

Confirmation on EU level if compliance with sanctions lists, AML/KYC requirements and other regulatory requirements qualifies as a "critical or important function" as defined in Article 3(22) DORA would be welcome.

14.3.2. Smart contracts will normally qualify as "ICT asset"

Smart contracts[221] are an essential element of blockchain projects and crypto-asset service providers and often manage assets and transactions. Blockchain projects can use a wide variety of smart contracts depending on the nature and the complexity of the application.

Smart contracts will normally qualify as 'ICT asset' in the sense of Article 3(7) DORA.

Financial entities will therefore need to assess which smart contracts that are deployed as part of their operations and services, or when possible before their deployment, could lead to ICT-risks in the sense of Art. 3(5) DORA.

Which smart contracts could lead to such ICT-risks depends on how the smart contract(s) will be used. Smart contracts that control assets/funds and transactions would likely require specific attention from a DORA perspective but serious incidents could also arise from other smart contracts. From a risk management point of view, the most critical smart contracts should be analysed first, but other smart contracts can also bear risks and should also be risk-assessed.

In accordance with the need for ongoing DORA compliance, smart contract updates should normally require an updated assessment under DORA, particularly if changes are significant. Even in the absence of updates, periodic assessments may still be necessary.

[221] According to Article 2(39) of Regulation (EU) 2023/2854 (Data Act) 'smart contract' means a computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering.

14.3.3. Standards for smart contracts

Regulation (EU) No 1025/2012 refers to different types of standards[222] and provides a legal basis to use European standards for products and services and identify ICT technical specifications. The use of these standards is voluntary. However, compliance with standards adopted by the European Standardization Organizations (CEN/CENELEC and ETSI) in accordance with regulation 1025/2012 and international standards adopted by international standardisation bodies (ISO, IEC and ITU) can be required in public procurement requests within the European Union.[223]

There are currently no technical standards adopted by the European Standardization Organisations that specifically focus on smart contracts.[224] ETSI and CENELEC have dedicated committees for DLT, blockchain and smart contracts.[225]

There is a difference between standards in accordance with regulation 1025/2012 and industry technical specifications which are outside the scope of regulation 1025/2012. Guidance if/to what extent compliance with such industry technical specifications relating to security of DLT solutions[226] and smart contracts[227] are enhancing compliance with DORA requirements would be helpful. For smart contracts this could possibly be part of the implementation of Article 36

---

[222] Article 2(1) Regulation (EU) No 1025/2012 refers to "international standards adopted by International standardisation bodies (ISO, IEC or ITU), European Standards (including harmonized standards) adopted by European standardization organization (CEN, CENELEC or ETSI) and national standards adopted by national standardization bodies.

[223] Reference is made to Recital (30) of Regulation No 1025/2012 which also refers to the possibility to refer to national standards in the event that European standards or international standards do not exist.

[224] Chapter III section 11 (Article 45k and 45l) of the eIDAS2 regulation with respect to electronic ledgers lays down a framework for "qualified" electronic ledgers. On the basis of Art. 45l(3) a list of reference standards and where necessary specifications and procedures will be established by the European Commission by means of implementing acts. According to Article 45l 1(a), qualified electronic ledgers are created by one or more qualified trust service provider or providers which will likely not be the case for most public permissionless DLT networks. See also Chapter 11, paragraph c) of the 1st cohort best practices report.

[225] After completion of the eIDAS 2 focused dialogues for the 2nd round ETSI published the draft working document ETSI TR 119 540 V0.0.6 (2025-02) titled *"Electronic Signatures and Trust Infrastructures (ESI); Standardisation requirements for Smart Contracts based on Electronic Ledgers"*: ETSI DRAFT TR_119_540v0.0.6-public.pdf. The draft document defines standardisation issues for Smart Contracts, as defined in the Data Act and based on Electronic Ledgers as defined by eIDAS 2.

[226] Examples of industry technical specifications for resilience testing are for instance:

- PCI DSS - https://east.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment - https://csrc.nist.gov/pubs/sp/800/115/final
- OWASP (Open Web Application Security Project):
  - Top 10: OWASP Top Ten
  - ASVS (Application Security Verification Standard): OWASP ASVS
  - MASVS (Mobile Application Security Verification Standard): OWASP MASVS
  - Mobile Security Testing Guide (MSTG): OWASP MSTG
  - Web Security Testing Guide (WSTG): OWASP WSTG
- PTES (Penetration Testing Execution Standard): PTES Official Site
- MITRE ATT&CK Framework: MITRE ATT&CK
- SANS Institute Resources:
  - Conducting a Penetration Test on an Organization: SANS Penetration Testing
  - Network Application Security Assessment and Ethical Hacking: SANS Ethical Hacking
  - Top 25 Common Weakness Enumerations (CWE): SANS Top 25
- Open Source Security Testing Methodology Manual (OSSTMM): OSSTMM

[227] Examples of industry technical specifications for smart contracts are for instance:

- EEA EthTrust Certification - https://entethalliance.org/specs/ethtrust-sl/v2/;
- OWASP Smart Contract Security Verification Standard - https://owasp.org/www-project-smart-contract-security-verification-standard/
- CCSS - https://cryptoconsortium.org/standards-2/

of the Data Act (Essential requirements regarding smart contracts for executing data sharing agreements).[228]

14.3.4. Requirements for testers for carrying out TLPT

DORA lays down regulatory requirements regarding testing of ICT tools and systems, including frequency and advanced testing by means of TLPT.[229] Financial entities, other than microenterprises, shall ensure, at least yearly, that appropriate tests are conducted on all ICT systems and applications supporting critical or important functions.[230] At least every 3 years advanced testing needs to be carried out by means of TLPT by certain entities, in particular financial entities operating in core financial services subsectors and playing a systemic role (e.g. payments, banking, and clearing and settlement), and less relevant for other subsectors (for example, asset managers and credit rating agencies).[231]

The ESAs[232] in agreement with the ECB have developed draft regulatory technical standards in accordance with Article 26(11) DORA (TRS on TLPT)[233] specifying elements related to TLPT's in accordance with the TIBER-EU framework.[234]

According to Article 27 of DORA, financial entities shall only use testers for the carrying out of TLPT, which possess specific characteristics. Among the qualifications, article 27(c) states that TLPT testers must be *"certified by an accreditation body in a member state or adhere to formal codes of conduct or ethical frameworks"*. If internal testers are used, external testers need to be contracted every three tests.

Although member states may not have established a certification mechanism for TLPT testers, such testers can therefore also adhere to *"formal codes of conduct or ethical frameworks"*.

When a financial institution wants to conduct a TLPT test, it can choose a provider to perform a TIBER test.[235] The TIBER authority may determine, for reason, that the provider is not suitable for that particular test. In other instances, the financial institution may conduct the TLPT test privately to enhance its cybersecurity, without it being a TIBER test.[236]

Not only the technical requirements but also the organisational requirements are relevant. Reference is made to the RTS on TLPT. For example, the Spanish TIBER-ES implementation guide states: "*It is crucial that providers and their staff are sufficiently independent of the entity being tested, to ensure the objectivity of the test results. They must also have enough credited experience and skills for the proper and safe execution of the tests. […] The requirements in*

---

228 Article 36(5) Data Act refers to a request from the European Commission for one or more harmonised standards to be drafted by European standardisation organisations regarding essential requirements for smart contracts for executing data sharing agreements that satisfy the essential requirements laid down in Article 36(1) Data Act for such smart contracts. A smart contract that meets such harmonised standards or relevant parts thereof shall be presumed to be in conformity with the essential requirements laid down in Article 36(1) Data Act (Article 36(4) Data Act).

229 Article 24 - 27 DORA.

230 Article 24(6) DORA.

231 Article 26(1) DORA. Under DORA, it is compulsory across the EU for the financial entities in scope to undergo TLPTs at a frequency chosen by the TLPT authority or the competent authority according to the Member State implementation of Articles 26(9) and 26(10) of DORA authority (every three years in general) (see draft RTS mentioned in footnote 18, paragraph 12).

232 EBA, EIOPA and ESMA.

233 Joint Regulatory Technical Standards specifying elements related to threat led penetration tests, published on 17 July 2024 (link). These RTS on TLPT still need to be endorsed by the EC.

234 What is TIBER-EU?

235 https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html;

236 The relationship between the TIBER and DORA TLPT frameworks is explained in paragraph 2.2 of the Final Report of the ESAs and in recital 1 of the draft RTS specifying elements related to threat led penetration tests, published on 17 July 2024 (link): *"This Regulation has been drafted in accordance with the TIBER-EU framework and mirrors the methodology, process and structure of TLPT as described in TIBER-EU. Financial entities subject to TLPT may refer to and apply the TIBER-EU framework as long as that framework is consistent with the requirements set out in Articles 26 and 27 of Regulation (EU) 2022/2554 and this Regulation."*

terms of independence, experience and agreements with providers are described in the TIBER-EU Services Procurement Guidelines published by the ECB." TIBER-EU Service Procurement Guidelines are published on https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.el.pdf

In addition, certification by an accreditation body does not replace or mitigate the other requirements for testers laid down in Article 27 DORA. The term "accreditation body" used in Article 27 DORA is not defined in this regulation but refers to national accreditation bodies in the individual Member States. A list of the national accreditation bodies which have been appointed is not (yet) published. The national authorities responsible for the implementation of TIBER-EU or the national cybersecurity agencies could possibly provide guidance.

14.4. Areas for Further Clarification & Dialogue Topics for the Next Cohorts

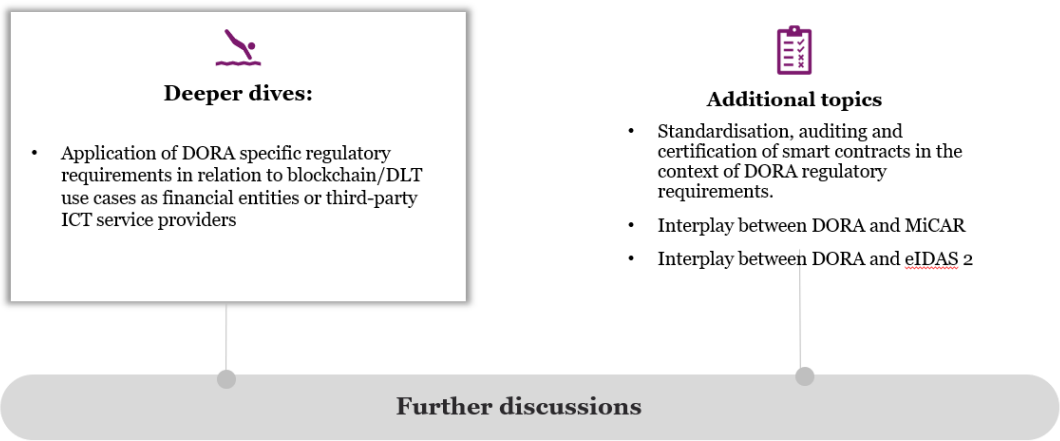
Several areas for further clarification and regulatory dialogue were identified during the dialogue meetings.

Deeper dives

- Interpretation of "critical or important function" as defined in Article 3(22) DORA in particular in respect of Blockchain/DLT solutions that enhance compliance with relevant regulations.
- Application of DORA specific regulatory requirements by Blockchain/DLT solution providers that qualify as "financial entities".
- Application of DORA specific regulatory requirements by "financial entities" that use Blockchain/DLT solutions provided by ICT third-party service providers.

Additional topics:

- Standardisation, auditing and certification of smart contracts in the context of DORA regulatory requirements.
- Interplay between DORA and MiCAR
- Interplay between DORA and eIDAS 2



15. Scope and delineation MiFID & MiCAR

15.1. Introduction

The focus of this chapter is the scope and delineation between MiFID and other financial sector regulation and MiCAR. As such this chapter provides the basis for the subsequent chapters which are more focused on specific financial regulatory areas.

Sope and delineation between financial sector regulation and MiCAR were also an important regulatory focus area in the 1st round of dialogues. Reference is made to chapter 13 and 14 of the 1st cohort best practices report.

Some elements of these chapters serve as a starting point for the 2nd round of dialogues and are quoted below in blue.

Report:[237]

- *The issuing of or the rendering of services for third parties relating to a specific token might be subject to European regulatory regimes depending on the qualification as a financial instrument under national transposition(s) of MiFID II (Markets in Financial Instruments Directive)*[238] *or a crypto-asset subject to MiCAR (Markets in Crypto Assets Regulation).*[239]

- *MiCAR does not apply to crypto-assets that qualify as financial instruments as defined in Article 4(1), point (15), of MiFID II.*[240]

- *The concept of "financial instrument" is not defined in one single definition in MiFID II, but described in a list of instruments including "transferable securities" included in Annex I. MiFID II includes the following definition of 'financial instrument':*[241]
  - *'**financial instrument**' means those instruments specified in Section C of Annex I;*
  - *Section C of Annex I refers to "Transferable securities" and a range of other financial instruments.*
  - *Transferable securities are in turn defined in Article 4(44) MiFID II:*

  *'**transferable securities**' means those classes of securities which are negotiable on the capital market, with the exception of instruments of payment, such as:*

  (a) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;
  (b) bonds or other forms of securitised debt, including depositary receipts in respect of such securities;
  (c) any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures;

---

237 Chapter 13, Financial sector regulation & MiCAR – Scope and Delineation, 1st cohort best practices report (June 2024).
238 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast).
239 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.
240 Article 2 point (4) MiCAR
241 Article 4(15) MiFID II.

- *MiFID II is a directive that needs to be transposed in the national legislation of the Member States. These national laws are not fully harmonized.*[242] *As a result, there are still different national interpretations whether a token may qualify as security in each member state.*

- *MiCAR is a regulation and is directly applicable in the Member States. […]*

- *The definition of "crypto-assets" is laid down in Article 3(1) point (5) MiCAR:*
  - *'crypto-asset' means a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology;*
- *MiCAR does not cover all types of crypto-assets.*[243] *Non-Fungible-Tokens (NFTs) are outside the scope of MiCA under certain conditions set out in the regulation.*[244]

- *The MiCAR definition of crypto-assets is also distinct from the definition of 'DLT financial instrument' in the DLT Pilot Regime which refers to a specific subcategory of 'financial instruments":*[245]
  - *'DLT financial instrument' means a financial instrument that is issued, recorded, transferred and stored using distributed ledger technology;*
- *Whether a security token, currency token/cryptocurrency (e.g. a stablecoin) or a utility token or security token is subject to a certain regime (MiFID, MiCAR or neither) depends on the specific features of the respective token and must be determined on a case-by-case basis. An important first assessment to be made is if the token qualifies as a "financial instrument", such as a "transferable security" under the relevant national legislation by which MiFID II is transposed in national law.*[246] *If a specific token/coin qualifies as both, the MiCAR regime will not apply, but instead the MiFID II regime is applicable.*[247]

The ESMA Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments were published on 19 March 2025.[248] The purpose of these guidelines is to specify conditions and criteria for determining whether a crypto-asset should qualify as a financial instrument and therefore ensuring the common, uniform and consistent application of the provisions in Article 2(4)(a) of MiCA. Furthermore, these guidelines provide clarifications on certain features of utility tokens, NFTs and hybrid tokens.

15.2. National corporate law aspects on tokenization of shares and qualification of tokenized assets

The harmonized EU Legislation defines the categories of financial instruments but does not define precisely *the specific characteristics of every* single financial instrument that can be included in each category.[249] Therefore, in order to understand if a specific asset can be qualified as a financial instrument, in some cases, an analysis of the specific characteristics of

[242] Reference to ESMA consultation doc. Of 29.01.2024. See ESMA 29 January 2024, 'Consultation Paper On the draft Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments', ESMA75-453128700-52 (available via this link). The Guidelines were adopted and published 19 March 2025 see footnote 240.
[243] More specifically, the MiCA Regulation does not apply either to crypto-assets that qualify as deposits, funds (except if they qualify as e-money tokens), securitisation positions, non-life or life insurance products and pension products (Article 2(4) MiCAR).
[244] Recitals 10 and 11 MiCAR.
[245] Regulation (EU) 2022/858 of the European parliament and of the council of 30 May 2022 ("DLTR").
[246] Article 4(1)(15) MiFID (definition of financial instrument) in conjunction with Annex I, Section C, to MiFID II (reference to "transferable securities") and Article 4(1)(44) MiFID (definition of "transferable securities").
[247] Article 2(4)(a) MiCAR.
[248] ESMA 19 March 2025, 'Guidelines On the conditions and criteria for the qualification of crypto-assets as financial instruments', ESMA75453128700-1323 (available via this link).
[249] Reference is made to Chapter 14 of the 1st cohort best practices report.

the asset is required. Those characteristics can be either determined by law, or by technical functionality and contractual arrangements.

The Guidelines of 19 March 2025 on the conditions and criteria for the qualification of crypto assets as financial instruments will not change the definition of financial instrument in MiFID 2 as transposed into national legislation.

15.3. Step-by-step analysis for the classification of tokenized instruments

The question if the tokenized quota is regulated by financial sector regulation is determined by the following steps:

a. Is the tokenized quota a financial instrument in the sense of MiFID2?
b. If not, are the tokenized quote a crypto asset in the sense of MiCAR? Or an Investment Fund in the sense of the AIFMD?
c. If regulation laid down in the MiFID2, MiCAR and the AIFMD is not applicable financial products and services could still fall under national legislation covering specific non-EU regulated types of financial products or services.[250]

As part of the analysis in the previous paragraph the following line of reasoning could be helpful.

A perfect digital twin of an original instrument[251], in accordance with applicable national legislation, would normally not change the qualification of the instrument under applicable law. Therefore, the perfect digital twin of a tokenized instrument would not qualify as a financial instrument, if the original instrument does not qualify as a financial instrument under national law.

However, if a tokenized instrument is not a perfect digital twin of the original instrument, the qualification of the tokenized instrument could be different from the qualification of the original instrument depending on the technical and contractual characteristics:

a. If the original instrument is not a financial instrument because the asset is not fungible/transferable, the tokenized instrument could also be not fungible/transferable or could nevertheless be fungible/transferable depending on the technical and contractual characteristics of the tokenized instrument.
b. If the original instrument is a financial instrument, the tokenized instrument could nevertheless not be a financial instrument depending on the technical and contractual characteristics which could imply that the tokenized instrument is not transferable and/or non-fungible.
c. The qualification if the token is a financial instrument needs to be made independently from the underlying asset with the outcome in no way being predetermined by the underlying asset.

If the tokenized instrument does not qualify as a financial instrument, the further assessments under MiCAR/AIFMD and national legislation referred to above become relevant.

The differences in national legal frameworks and obstacles for asset tokenization in Member States will likely be analysed in more detail in a Study that is contracted by the European Commission, Call for tenders EC-FISMA/2024/OP/0003.[252]

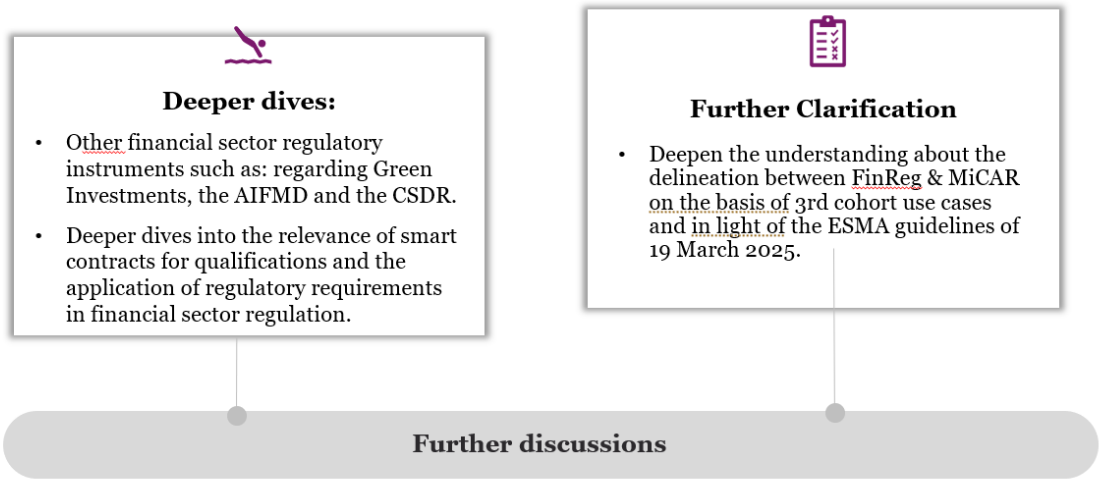
As the qualification of tokenized instruments will require analyses on a country level, this could possibly be discussed in more detail on a country level, for instance in a national sandbox.

---

[250] Reference to national law examples in Italy and Germany.
[251] A perfect digital twin of the original instrument would be the digital equivalent of the original participation with exactly the same rights (a.o. governance, voting rights, dividend) attached to it.
[252] EU Funding & Tenders Portal

15.4. Areas for further clarification and dialogue

Additional financial sector use cases will be part of the next cohort dialogues. This will provide the opportunity to deepen the understanding about the delineation of the different legal regimes also in light of the ESMA guidelines of 19 March 2025.



16. Use of the DLT Pilot Regime

16.1. Introduction

The DLT Pilot Regime Regulation (**"DLTPR"**)[253] became applicable on 23 March 2023. In a letter to ESMA dated 3 May 2024, the European Commission clarified that the DLTPR has no expiry date:[254]

> *"There is one frequent question on the DLT Pilot Regime that I wish to address in this letter. You note that a major source of hesitation for potential applicants is a perceived uncertainty about the duration of the DLT Pilot Regime. Allow me to clarify that there is no expiration date for the DLT Pilot Regime. As with any other EU legislation, changes to the Regime – and this includes its termination - may only occur if, in accordance with its Article 14(2), the Commission were to submit a new legislative proposal and if that proposal were to be agreed by the co-legislators. In other words, if no proposal is made and adopted to amend the Regime, the framework will continue to apply in its current form. And at this stage, no proposal to terminate the regime is envisaged. The Commission remains fully committed to the Regime and its policy objective of fostering DLT-based innovation in financial markets."*

The objective of the DLTPR is to promote the use of DLT providing the possibility to apply for exemptions from certain specified MiFID II[255] and/or CSDR[256] requirements which are incompatible with a DLT-based infrastructure. Requirements and exemptions regarding

DLT MTFs[257], DLT SSs[258] and DLT TSSs[259] are laid down in Articles 4, 5 and 6 DLTPR respectively.

Further information on the DLTPR, including guidelines, Q&As and reports, can be found here: ESMA - DLT Pilot Regime page

In addition, some Member States facilitate the EU DLT Pilot Regime by corporate law amendments in national legislation.[260]

Example from the 1st cohort best practices report: Finland:

[253] Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU.

[254] Letter from the European Commission on the DLT Pilot Regime Implementation

[255] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.

[256] Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (Central Securities Depository Regulation).

[257] Exemptions for DLT MTFs are possible from certain regulatory requirements laid down in Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU ("**MiFID II**") and Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 ("**MIFIR**").

[258] Exemptions for DLT SSs are possible from certain regulatory requirements laid down in the Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 ("**CSDR**").

[259] Exemptions for DLT TSSs are possible from certain regulatory requirements laid down in MiFID II/MIFIR and the CSDR.

[260] An example in Finnish law was discussed in the 1st best practices report.

The EU DLT Pilot Regime Regulation is facilitated in Finland by corporate law amendments on a national level enabling the registration of shares in a limited liability company in a DLT based settlement system instead of a traditional book-entry securities system. This amendment goes beyond the change of the definition of "financial instrument" following the amendment of MiFID II in accordance with Article 18 of the EU DLT Pilot Regime Regulation.

Italy: Decree-Law 25/2023

For instance, Italian legislation on the one hand implements the DLT Pilot Regime in the Italian legal system (by adapting certain rules of Italian company law) and, on the other hand, provides for a new regime for the issuance and circulation in blockchain of financial instruments governed by Italian Law. In fact, the European DLT Pilot Regime regulates the issuance and circulation in digital form (DLT/blockchain) of certain financial instruments like shares, bonds and fund units intended to be traded on trading venues governed by the European Law that will be specifically authorised for the purpose (DLT trading venues). Within these trading venues, securities will not be subject to the obligation to register with a central depositary (as is the case under the CSDR Regulation) but are created and transferred directly in the DLT environment. These DLT trading venues may be operated by financial intermediaries and central depositories.

The Italian legislation allows the issuance and circulation in a DLT environment of digital financial instruments (like shares, bonds and units in collective investment funds) governed by Italian Law, not intended to be traded on trading venues governed by European law.

For digital financial instruments governed by Italian Law not intended to be traded on trading venues governed by European Law, Italian legislation provides for the establishment of a digital register for the issuance and circulation in the DLT environment.

16.2. Application for DLT Pilot Regime exemptions

If trading facilities and/or settlement systems want to operate a DLT-based infrastructure as a DLT MTF, DLT SS or DLT TSS, exemptions from such MiFID II and/or CSDR requirements will not be automatically granted by supervisory authorities. Some of the regulatory requirements may be incompatible with DLT infrastructures or with some of the objectives pursued by the EU legislator with the adoption of the DLTPR, but the applicant should provide evidence regarding counterbalancing measures to address the risks associated with the exempted obligations, taking account of the underlying principles and through a case-by-case analysis assess. The operator should comply with the requirements of the DLTPR and implement the compensatory measures requested by the competent authority to meet the objectives pursued by the requested exempted provisions, before being granted an exemption by the competent authority. In addition, the operator should provide explanation of why the exemptions are proportionate to, and justified by, the use of DLT.

By way of example: the applicant can apply for an exemption from the reconciliation and record keeping requirements laid down in Articles 37/38 CSDR, but it should be demonstrated why these requirements cannot be met and which counterbalancing measures will be taken.

Whether or not these criteria are met by the applicant appears to be a topic for ESMA. See recital (44):

> *"A specific permission granted to an operator of DLT market infrastructure should broadly follow the same procedures as those for authorisation under Regulation*

(EU) No 909/2014 or Directive 2014/65/EU. However, when applying for a specific permission under this Regulation, the applicant should indicate the exemptions it is requesting. Before granting a specific permission to a DLT market infrastructure, the competent authority should provide ESMA with all relevant information. Where necessary, ESMA should issue a non-binding opinion on the exemptions requested or on the adequacy of the distributed ledger technology for the purposes of this Regulation. Such a non-binding opinion should not be deemed to be an opinion within the meaning of Regulation (EU) No 1095/2010. ESMA should consult the competent authorities of other Member States when preparing its opinion. With its non-binding opinion, ESMA should aim to ensure investor protection, market integrity and financial stability. In order to ensure a level-playing field and fair competition throughout the internal market, ESMA's non-binding opinion and guidelines should aim to ensure the consistency and proportionality of the exemptions granted by different competent authorities in the Union, including when evaluating the adequacy of different types of distributed ledger technology used by operators for the purposes of this Regulation."

The aim of the DLTPR provisions is to protect investors and ensure market integrity and applicants are therefore subject to a comply-or-explain mechanism. Also considering that in the application phase the counterbalancing measures are not yet implemented, it is recommended that the information that is provided as part of the application is as clear and objective as possible in order to support the assessment by the competent authorities and facilitate a supervisory dialogue about important elements of the application for exemption.

In addition to a plain and detailed description, a risk-matrix might be part of the application, summarising the requirements for which a waiver is requested, the risks that may occur as a result of such waiver or by the use of a DLT and which alternative measures are proposed to counterbalance such risks.

Exemptions that are requested: requirements to be waived	Risks that are addressed by these requirements	Proposed alternative measures to counterbalance the requirement that would be waived
Art. X DLTPR in connection to Art. Y CSDR / Art. Z MiFID II	Risk 1	• Measure(s) A, (B)

In 2024, two entities have been authorized in accordance with the DLTPR. On 11 October 2024, ESMA announced that CSD Prague (Centrální depozitář cenných papírů, a.s.) is the first ever licensed operator as a DLT SS. 21X AG was the second operator to receive a DLT Pilot Regime authorisation (as a DLT TSS) on 3 December 2024. ESMA's register of Authorised DLT Market Infrastructures includes for each operator a 'list of exemptions granted under DLTPR'.[261] Without mentioning any counterbalancing measures applied, the exemptions for both operators include inter alia:

- Article 6 CSDR on measures to prevent settlement fails;
- Article 7 CSDR on measures to address settlement fails;

[261] This reflects the status of 4 April 2025. See for the most recent list of authorised parties https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/dlt-pilot-regime under 'Authorised DLT Market Infrastructures'.

- Article 35 CSDR on communication procedures with participants and other market infrastructures;"
- Article 38 CSDR on the segregation of assets;
- Article 39 CSDR on settlement finality;
- Article 40 CSDR on cash settlement.

Further, it is notable that 21X AG is, *inter alia*, exempt from Article 2(1) No 4 CSDR on 'dematerialised form', Article 2(1) No 9 CSDR on 'transfer order', Article 2(1) No 19 CSDR on 'participant', Article 2(1) No 28 CSDR on 'securities account', and Article 3 CSDR on 'book-entry form'.

16.3. Outsourcing of services by a DLT SS/DLT TSS provider as part of an application for a DLTPR exemption

The exemption of Article 5(4) of the DLTPR (outsourcing of a CSDR core service) is solely applicable to CSDs operating a DLT SS but not to investment firms operating a DLT MTF (which is covered by Article 4 DLTPR). However, an investment firm or CSD operating a DLT TSS can benefit from the exemption of Article 5(4) DLTPR due to the references in Article 6(1) and 6(2) DLTPR. Such exemption is limited to the provisions recalled by Article 5(4) (Article 19 CSDR in relation only to the outsourcing of a core service to a third party as defined by CSDR).

Outsourcing by CSDs[262] of core services[263] is possible with authorisation under the CSDR (Art. 19 CSDR).

- The authorisation requirement to perform core services as defined in the CSDR is laid down in Article 16 CSDR. The possibility to obtain an exemption to perform such core services is laid down in Article 5 and Article 6 DLTPR.
- The authorisation requirement to outsource core services as defined in the CSDR is laid down in Article 19 CSDR. The possibility to obtain an exemption to outsource such core services is laid down in Article 5(4) DLTPR and Article 6(2) DLTPR.

In order to assess if core services are outsourced and if the exemption to outsource core services could be obtained, it should be carefully considered what aspects of the activities are outsourced by the DLT SS/DLT TSS operator and which activities are taking place on- and off-chain to determine if/to what extent the regulatory requirements (such as the CSDR and the DLTPR) are applicable and which possible exemptions under the DLTPR could be relevant.

16.4. Areas for further clarification & dialogue

A further dialogue regarding the application of the DLTPR in relation to different DLT use cases would be helpful as there is still relatively limited experience with this still novel regulatory instrument.

[262] Definition of CSD in Article 2(1)(1) CSDR: A settlement service and a notary service AND/OR a central maintenance service.

[263] Core Services in Annex Section A CSDR: 1) notary service, 2) central maintenance service, 3) settlement service.

Some aspects for further clarification are mentioned in ESMA's letter of 3 April 2024[264] such as in relation to innovative solutions for cash settlement, the use of self-hosted wallets and the scope and the thresholds of admitted DLT financial instruments.

[264] ESMA75-117376770-460 Letter to EU Institutions on DLT Pilot Regime

17. Compliance with MiCAR

17.1. Introduction

The 2nd round of dialogues provided to opportunity to make a deeper dive into MiCAR related topics: scope, application and exemptions. Some elements were discussed during the 1st round of dialogues. Reference is made to chapter 13 of the 1st cohort best practices report.

Some elements of this chapter serve as a starting point for the 2nd round of dialogues with a MiCAR focus and are quoted below in blue.

17.2. MiCAR – regulatory framework

MiCAR's primary objective is to create legal certainty for crypto-asset markets within the EU legal framework, laying down harmonised organisational and conduct requirements for market participants as well as prudential rules for issuers of certain types of crypto-assets (namely e-money tokens and asset-referenced tokens), while introducing specific investor protection provisions and regulating the providers of crypto-asset services. The regulation of e-money tokens and asset-referenced tokens issuers applies since 30 June 2024; the regulation of crypto-asset service providers and issuers of other crypto-assets than e-money tokens and asset-referenced tokens since 30 December 2024.

Transferability and fungibility are two different aspects of a token and should not be mixed up. While the transferability of a token determines if a token qualifies as a crypto-asset as defined in MiCAR, the question whether a crypto-asset is non-unique and fungible determines if the requirements under MiCAR are applicable. The awareness of the user that a service provider makes use of DLT appears not to be a criterion under MiCAR for the qualification if a token qualifies as a crypto-asset.

MiCAR has two kinds of exemptions. First of all, certain crypto-assets are excluded from the scope of MiCAR. This includes, for example, financial instruments under MiFID II as well as crypto-assets that are unique and non-fungible. The second type of exemptions applies to crypto-assets generally in scope of MiCAR but releases in particular issuers from certain obligations (e.g. the publication of a crypto-asset white paper). This second type of exemptions , for example, applies to crypto-assets that are offered for free.

Although some physical or non-blockchain based products or services are not in scope of financial regulation, their digital blockchain based tokenized twins (if, among others, transferable and non-unique and fungible), based on the letters of the definition of MiCAR of crypto assets, are being classified as crypto-assets and fall under MiCAR regulation. Based on various aspects of these tokens, although classified as crypto-asset, exemptions within MiCAR are possible if the relevant conditions are met.

Reference is made to ESA’s flowchart below for the assessment whether a token is a crypto-asset under MiCAR which guides through the relevant questions to assess MiCAR applicability.

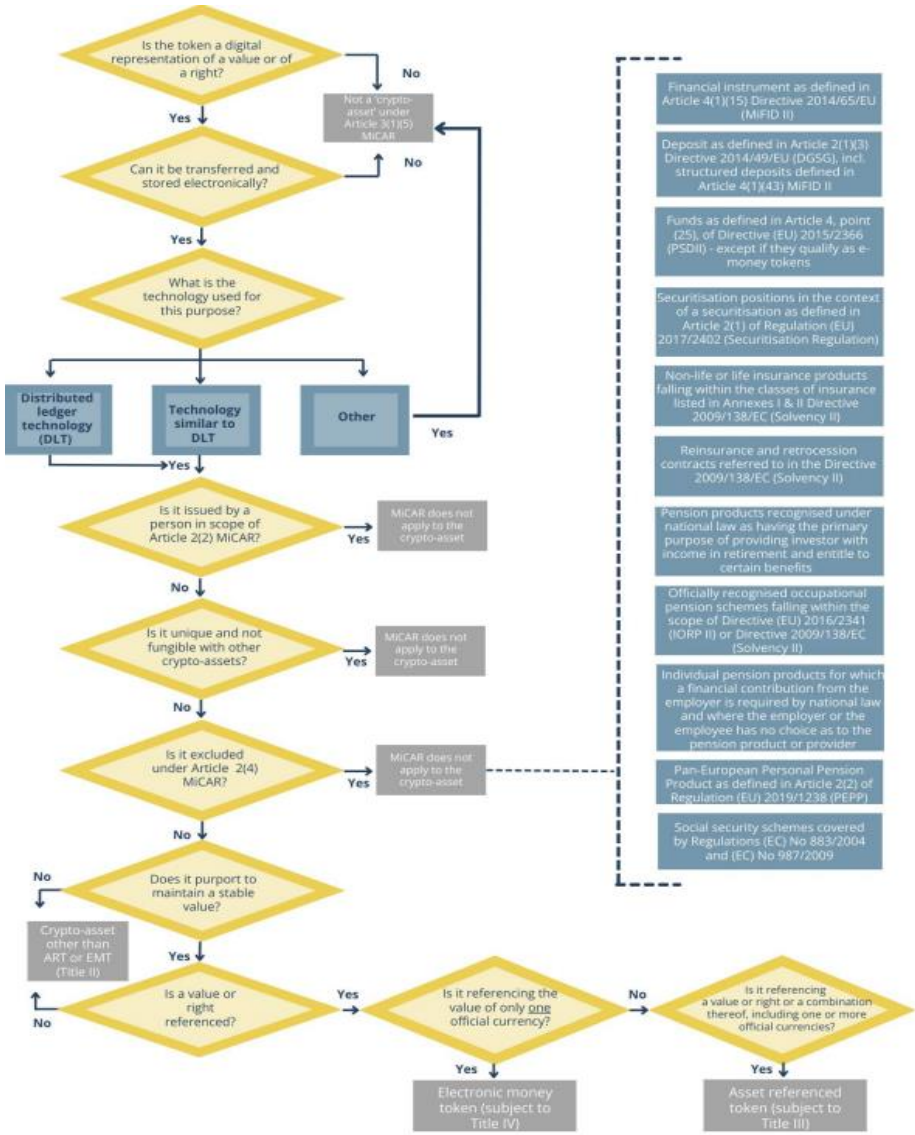


Figure 1 – ESA flow chart to determine the classification of a crypto-asset[265]

17.3. Transferability – best practices and lessons learned

The term "crypto-asset" is defined in Article 3(1)(5) MiCAR: *"Crypto-asset' means a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology."*

Transferability is a key element in this definition of "crypto-asset". If a digital representation of a value or of a right is not transferable, it does not qualify as crypto-asset under MiCAR.

In addition, the ESAs provide guidance in the Guidelines on templates for explanations and opinions, and the standardised test for the classification of crypto-assets, published on 10th December 2024.[266] Reference is made to paragraph 19 of these Guidelines: *"A token may be considered 'non-transferable' only where at least the following conditions are satisfied (i) the*

[265] ESA, 'Final Report – Guidelines on templates for explanations and opinions, and the standardised test for the classification of crypto-assets, under Article 97(1) of Regulation (EU) 2023/1114', 10 December 2024, JC 2024, 28, p. 30.

[266] The Guidelines are available through: https://www.esma.europa.eu/sites/default/files/2025-03/JC_2024_28_Guidelines_on_explanations_and_opinions__and_the_standardised_test_for_crypto-assets_under_MiCA.pdf

token is accepted only by the issuer or offeror, and (ii) there is no technical possibility for the token to be transferred by a holder to persons other than the issuer or offeror (recital (17) of Regulation (EU) 2023/1114).“

Contractual limitation in transferability or the use of whitelists alone do not imply that a token is non-transferable. If the tokens can only be transferred with the permission of the issuer, this is on its own not a sufficient criterion to exclude transferability. The technical possibility will be decisive. Transferability, however, is excluded if the token can only be re-transferred to the issuer and the issuer burns the token and, at the same time, issues a new token to another user.

17.4. Non-uniqueness and Fungibility – best practices and lessons learned

Report:[267]

- *The term non-fungible tokens (NFT) is often used in relation to crypto assets and MiCAR. However, in the context of MiCAR the use of this term is confusing as in principle only fungible tokens are within scope of MiCAR. The confusion is caused by the fact that based on the technology used, e.g., tokens using the ERC 721-protocol, usually presume the non-fungibility of that token due to the technical characteristics. However, the legal assessment if a token is non-fungible is not determined on the basis of this technical characteristic alone.*

- *Whether a token is “fungible” needs to be determined on the basis of the assessment of legal fungibility and not only on the basis of the technical characteristics.*

If a crypto-asset is unique and non-fungible, it is excluded from the scope of MiCAR (Article 2(3) and Recital (10) and (11) of MiCAR).

To assess the fungibility of a token it is important to assess the fungibility of the assets or rights represented (recital 11). Therefore, the conclusion "fungible" or "non-fungible" will also depend on the fungibility of the underlying assets or rights.

The fungible/non-fungible nature of a token requires a case-by-case assessment. A crypto-asset can be unique and non-fungible for instance if it relates to a specific seat in a certain row in a concert hall; it will likely be fungible if it relates to the general admission to a club/event/location. It is difficult to draw the line between fungible and non-fungible (for instance: are the 5 seats in VIP box no. 2 for a certain date and time fungible or non-fungible?). Fungibility therefore does not provide a unified solution for concert tickets.

As mentioned, fungibility needs to exist in relation to the right represented. The right to sit on one seat is unique while the right to sit in a box of five seats could qualify as fungible (with the other four rights to sit in the box). This differentiation is complex and not easy to understand. Practical guidance would be welcome.

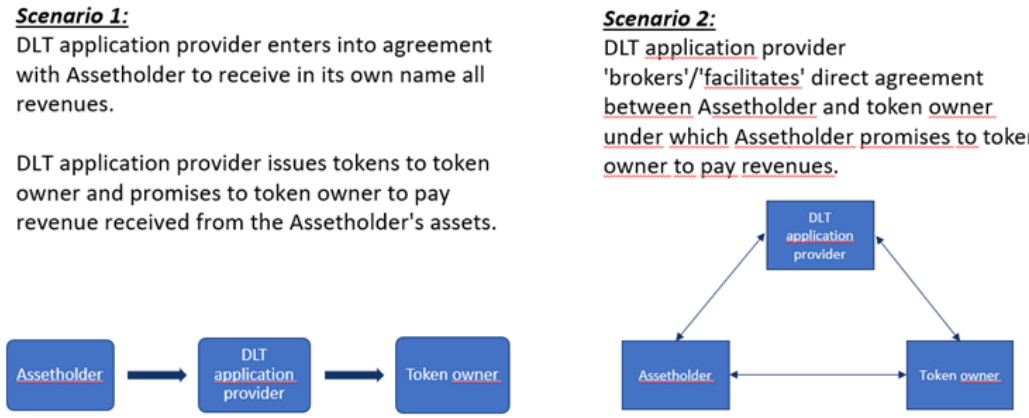
17.5. Applicability of MiCAR – who is the issuer?

Summary of findings in the report[268]

- *The main indicator for the issuer is the person who is responsible for fulfilling the (payment) obligations linked to the instrument. This assessment will depend on the set up and the contractual relations. In the graph below, the DLT application provider would*

[267] Chapter 13, Financial sector regulation & MiCAR – Scope and delineation, 1st cohort best practices report (June 2024).
[268] Chapter 13, Financial sector regulation & MiCAR – Scope and delineation, 1st cohort best practices report (June 2024).

most likely be qualified as the issuer and offeror in scenario 1, while in scenario 2, depending on the exact services offered, the DLT application provider could be qualified as service provider and depending on the service as offeror.



Fundamentally, the issuer is an entity to which persons in possession of crypto-asset have a claim. The issuer can be a different person from the person who programmed and controls the token smart contract. Technical service providers may offer their assistance to issuers making the issuance in the name of the issuer technically possible.

17.6. Exemptions from certain MiCAR requirements – best practices and lessons learned

As stated in the introduction to this chapter, MiCAR provides for exemptions from certain requirements even if the crypto-asset is in MiCAR's scope of application.
An offeror can make several offers to the public of crypto-assets at the same time if the crypto-assets are sufficiently distinct. Based on this, the exemption under Article 4(2)(b) of MiCAR likely applies per offer of crypto-assets and not per issuer:[269]

a. Article 4(2)(b) of MiCAR refers to an offer to the public of a crypto-asset. Therefore, the exemption likely applies to the offer of certain tokens and not to the business model;
b. The interpretation of the term "offer" under MiCAR should likely be understood in the same way as in the Prospectus Regulation.

A crypto-asset (utility token) representing a concert ticket can benefit from the exemption for utility tokens providing access to a good or service that exists or is in operation even if the concert is in some future. This does not apply if the crypto-asset issuance/offering has the purpose to finance the concert in first place (e.g. the fundraising to build the concert hall).

A 'white label' service provider might offer services in their own name and take the regulatory burden to comply with the applicable regulatory measures, such as the white paper obligation. This would allow businesses to benefit from the services of a third party without being treated as issuer or offeror themselves. Such possibility is effectively allowed under MiCAR (in this respect, please see Articles 4, 5 and 6).

A service provider who would offer services in its own name to end-users might provide not only custody and administration and transfer services for crypto-assets, but also other services

[269] Article 4(2)(b) MiCAR: "*Paragraph 1, points (b), (c), (d) and (f), shall not apply to any of the following offers to the public of crypto-assets other than asset-referenced tokens or e-money tokens: […] (b) over a period of 12 months, starting with the beginning of the offer, the total consideration of an offer to the public of a crypto-asset in the Union does not exceed EUR 1 000 000, or the equivalent amount in another official currency or in crypto-assets;".*

such as the exchange of crypto for funds. For the latter service, the service provider cannot benefit from the exclusion in Article 4(5) MiCAR and requires an authorization to provide crypto-asset services.

17.7. Regulated/unregulated custody – best practices and lessons learned

Custodial services for tokens that are not crypto-assets and/or fall under an exemption under Article 4(5) MiCAR (unless in the cases expressly set out herein) do not qualify as a CASP governed by MiCAR.

The question is if the non-regulated custodial service could become a regulated custodial service solely because there is a risk that regulated tokens are sent to the wallet which cannot be prevented by the hosted wallet provider.

A distinction should be made between permissioned and permissionless blockchains in the sense that permissioned blockchains provide more possibilities to control for which tokens a wallet is used than permissionless blockchains.[270]

However, many use cases operate on permissionless blockchains (with open standards/protocols/services, standard smart contracts and open-source software). When operating on a permissionless blockchain, the hosted wallet provider cannot prevent that crypto currencies or tokens are sent to an account.

The mere fact that a wallet is operated on a permissionless blockchain and therefore runs the risk of receiving regulated tokens which would instantly put the wallet provider within the scope of MiCAR could be considered as not proportionate, in particular under the following conditions:

- the hosted wallet providers prevent that such crypto currencies or tokens are visible for the account holders, and
- transaction requests for sending out such crypto currencies or tokens are not accepted (assuming that transactions are signed and sent by the account holders per asset), and
- the wallet providers explicitly exclude regulated tokens from entering the wallets in their T&Cs and do what they technically can to prevent this.

It could be argued that if these conditions are met, the wallet provider should not be considered as a regulated custodial service provider based on the principle of proportionality. That said, it would be appropriate requiring some confirmation by the EC or ESAs of this interpretation.

The question is what happens / should be done if the customer violates the contract and uses the wallet for regulated tokens. Probably a distinction should be made depending on the cause of the violation of the contract: a.o. a mistake by the holder, a reputational attack by a competitor, a deliberate violation? It appears that there is no guidance about how to deal with 'bad faith behavior' in connection with the use of wallets for unregulated tokens. Additional guidance would be welcome. Parties can also submit MiCAR related questions to ESMA to be included in the Q&A.

17.8. Gas/transaction fees

Some permissionless and public permissioned blockchains require gas/transaction fees for transfers of tokens. As the case may be, such gas/transaction fees might qualify as crypto-assets with no identifiable issuer and they do not fall within the scope of Title II, III or IV of MiCAR. However, custody services for gas/transaction fee tokens could still be governed by MiCAR (see Recital (22) of MiCAR).

[270] ISO 22739:2020(en), Blockchain and distributed ledger technologies — Vocabulary

An argument in support of the conclusion that the tokens used for payment of gas/transaction fees are not held in custody could be that the customer cannot do anything with the gas fees and that the use is solely at the discretion of the wallet provider.
It could be useful to explore if there are technical options (including which parties in the market could develop such options in a permissionless blockchain) to make sure that the gas/transaction fees never hit the wallet of the user if a service provider wants to allow free transfers of tokens based on permissionless and public permissioned blockchains (irrespective of whether qualifying as crypto-asset).

In view of the above, more clarity about the issue if (and under which circumstances) the payment of gas/transaction fees entails a regulated custody service under MiCAR would be welcome. This could be a question for ESMA, but it might also require a level one text amendment.

17.9. Applicability of PSD2 and EMD2 or MiCAR

Report[271]

- *Different aspects may be considered as part of the assessment of the exchange of tokens and if this could qualify as a payment service:*
  - *Not being involved in the payment between the customer and the service provider, not receiving any funds and if the service provider can accept the payment or not, could be indications not to qualify the use case as a payment service.*
  - *The role of the smart contract to complete the transaction between the service provider and the customer could also be relevant. Smart contracts created by and which benefit the owner/operator, could result in the owner/operator to be involved in service provisioning. In that case, smart contracts may act as an (automated) exchange, which may qualify as a payment service.*
- *Exchanging corresponding amounts (as required in the definition of money remittance) requires that funds are paid on both sides. A payment service necessitates that both directions of the transfer are in funds and if not, it is no payment service. If there is a transfer of a crypto-asset (other an EMT or ART) on one side, it is likely that there is no payment service. If there is a transfer of EMT, it is likely there is.*
- *Providing transfer services for crypto on behalf of clients can be considered as a crypto-asset service, regardless of whether it can be qualified as an exchange, and should therefore be licensed under MiCAR.*
- *Delineation between a payment service and a crypto-asset service also depends on qualification of certain stablecoins as e-money tokens or not, as these tokens are classified as funds. Further clarifications regarding qualification and categorization of stablecoins could provide more clarity here.*

[271] Chapter 13, Financial sector regulation & MiCAR – Scope and delineation, 1st cohort best practices report (June 2024).

	Token to pay a service is a Crypto-Asset other than an E-Money Token	Token to pay a service is an E-Money Token and therefore considered as Funds
Token to access a service is a Crypto-Asset	Crypto-asset <-> Crypto-asset ➔ *Exchange of CA for CA*	Crypto-asset <-> Funds ➔ *Exchange of CA for Funds* ➔ *Payment Service*
Token to access a service is not a Crypto-Asset	Service <-> Crypto-asset ➔ *Transfer services for CA on behalf of clients*	Service <-> Funds ➔ *Payment Service*

- *In relation to the qualification of tokens under MiCAR and the delineation between crypto-asset services and payment services, additional guidance on an EU level, for instance through a consultation by ESMA/EBA would be welcome.*

The assessment regarding the applicability of PSD2/EMD2 and MiCAR are to some extent interdependent. If tokens qualify as an EMT under MiCAR, such tokens will also qualify as "funds", because according to Article 48(2) MiCAR an EMT shall be deemed as e-money.

Consequently, PSD2 is applicable and therefore a PSP license may be required. The interplay between PSD2 and MiCAR is still an area where clarification would be welcome.[272] The interplay between PSD 2 and MiCAR will likely be clarified in PSD3[273] and the PSR.[274] In the meantime, further guidance from ESMA/EBA would be welcomed.

- Letter from DG FISMA to EBA in which DG FISMA referring to the diverging interpretations amongst Member States and exploring the possibility to issue an opinion in accordance with Article 9c of Regulation 1093/2010 ("No action letter"), with regard to the enforcement of the requirements on authorisation in PSD2 as regards services with EMTs provided by CASPs;[275] and

- Response from EBA to DG FISMA concurring with DG FISMA's findings and stating that EBA will assess the issues and aims to publish a response by April 2025.[276]

In view of the questions regarding the delineation between crypto-asset services and payment services, several examples were discussed in the 2nd round of dialogues:

  - E-vouchers do not qualify as e-money if they are not issued in receipt of funds and assuming that the DLT service provider who facilitates transactions pertaining thereto is not in the possession of any funds related thereto. Further, e-voucher tokens do not

[272] Reference made to the EBS 1st cohort best practices report, Chapter 13 under b).
[273] Progress of the legislative process regarding PSD3 (2023/0209(COD)) can be followed via this link: https://oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference=2023/0209(COD)
[274] Progress of the legislative process regarding PSR (2023/0210(COD))can be followed via this link: https://oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference=2023/0210(COD).
[275] See the letter from DG FISMA to EBA (https://www.eba.europa.eu/sites/default/files/2024-12/3225040c-5f3d-410f-9156-f06a43231938/Letter%20to%20EBA%20and%20ESMA%20on%20the%20interplay%20between%20MiCA%20and%20PSD2.pdf) and
[276] See the letter from EBA to DG FISMA: https://www.eba.europa.eu/sites/default/files/2024-12/ca287b45-8617-40bd-be1b-cc026a50a347/2024%2012%2010%20EBA%20response%20to%20Mr%20Berrigan%20re%20Interplay%20between%20MiCA%20and%20PSD2.pdf).

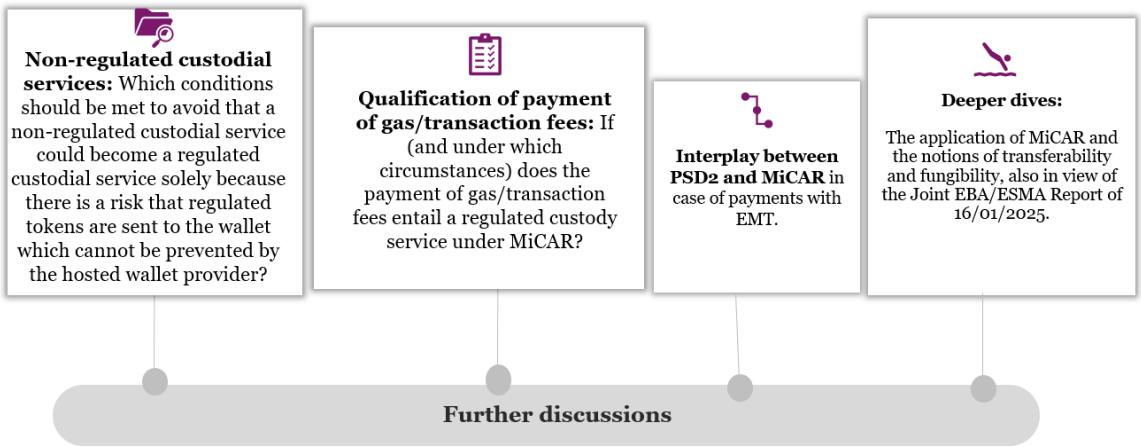
qualify as EMT's/funds if they do not meet the criteria for crypto-assets (e.g. transferability, see par. [xxx]) or if they do not purport to maintain a stable value by referencing the value of one official currency.

- A DLT service provider may prepare a SEPA file and submit it to the customer. As long as the DLT service provider does nothing in relation to the authorisation of such payment transaction with the customer's payment service provider, this is not a payment initiation service.

17.10. Areas for further clarification & dialogue

Several areas for clarification or further discussion were identified:

- **Deeper dives** into the application of MiCAR and the notions of transferability and fungibility, also in view of the Joint EBA/ESMA Report of 16/01/2025: ESMA75-453128700-1391 Joint Report on the recent developments in crypto-assets (Article 142 of MiCAR)
- **Non-regulated custodial services:** Which conditions should be met to avoid that a non-regulated custodial service could become a regulated custodial service solely because there is a risk that regulated tokens are sent to the wallet which cannot be prevented by the hosted wallet provider?
- **Qualification of payment of gas/transaction fees:** If (and under which circumstances) does the payment of gas/transaction fees entail a regulated custody service under MiCAR?
- **Interplay between PSD2 and MiCAR** in case of payments with EMT.



18. Application of the ECSPR

18.1. Introduction

The European Crowdfunding Service Provider Regulation (Regulation (EU) 2020/1503 – "**ECSPR**") regulates crowdfunding services[277], i.e., i) the facilitation of granting of loans or ii) the placing without a firm commitment basis as well as the reception and transmission of client orders of transferable securities and admitted instruments for crowdfunding purposes in each case via an online platform. Crowdfunding services are subject to an independent authorisation requirement.[278] Crowdfunding offers of more than EUR 5 million[279] are excluded from the scope of ECSPR. Crowdfunding service providers are exempted from the scope of Directive 2014/65/EU ("**MiFID 2**").[280]

The offer of transferable securities which exceed the threshold of EUR 5 million or which are offered via other services than crowdfunding services fall outside the scope of ECSPR. Such offerings are regulated by MiFID 2 and Regulation (EU) 2017/1129 (**"Prospectus Regulation"**).

18.2. Capital requirements - cumulative thresholds

The ECSPR and MiCAR include similar provisions on prudential or capital requirements to ensure that consumers and clients are protected against operational and financial risks related to crowdfunding and crypto-asset service providers. Additionally, this should safeguard the continuity of the business and prevent jeopardizing the interest of consumers and clients.[281]

The ECSPR requires all crowdfunding service providers to have at all times prudential safeguards in place of at least EUR 25.000 or, if higher, one quarter of the fixed overheads of the preceding year.[282] Meanwhile, the MiCAR introduced a layered approach introducing 'classes' with varying minimum capital requirements for different types of crypto-asset providers:

- Class 1: other services – minimum capital requirement of at least EUR 50.000;
- Class 2: custody and administration, exchange of crypto-assets for funds or for other crypto assets – minimum capital requirement of at least EUR 125.000;
- Class 3: crypto-asset trading platform– minimum capital requirement of at least EUR 150.000.[283]

Overlapping activities could lead to questions which prudential safeguards to adhere to. In case a service provider holds both, a MiCAR and ECSPR license, the overlap of prudential safeguards may be solved as follows in light of the applicable legislation:

Article 67(1) **MiCAR**	**Article 11(1) ECSPR**	**Potential solutions in case of overlapping activities**

[277] Defined in Article 2(1)(a) ECSPR.
[278] Article 12 ECSPR.
[279] Calculated in accordance with Article 1(1)(c) ECSPR.
[280] Article 2(1)p MiFID 2.
[281] See recital 24 and Article 11 ECSPR and recital 80 and Article 67 MiCAR.
[282] Article 11(1) ECSPR.
[283] Article 67(1) and Annex IV MiCAR. In accordance with Article 67(1) MiCAR, if the amount of one quarter of the fixed overheads of the preceding year exceeds the minimum capital requirement for a certain service, that amount should be adhered to.

(a) the amount of permanent minimum capital requirements indicated in Annex IV, ranging between EUR 150.000 (crypto-asset trading platform) or EUR 125.000;(custody and administration, exchange of crypto-assets for funds or for other crypto assets) and EUR 50.000 (other services)	*(a) EUR 25 000; and*	The minimal capital requirement is at least EUR 75,000 (50,000 + 25,000; or higher depending on whether the thresholds of Article 67 MiCAR are met) because this amount covers two seperate activities (crypto-asset services and crowdfunding services)
(b) one quarter of the fixed overheads of the preceding year, reviewed annually.	*(b) one quarter of the fixed overheads of the preceding year, reviewed annually, which are to include the cost of servicing loans for three months where the crowdfunding service provider also facilitates the granting of loans.*	The minimal capital requirement is at least one quarter of the fixed overheads of the preceding year of that company. If this calculation leads to an amount higher than the accumulated amount it would be under sub (a), such higher amount needs to be met. This threshold shall be calculated on to the entity as a whole regardless of the licenses that the company holds and not relate to the separate activities. This is because the costs are accounted for the company as a whole (for example personal costs, operating cost, marketing cost etc.) regardless how many licences it operates.

Prudential safeguards should be in the form of either own funds or an insurance policy. In relation to holding own funds as prudential requirements, own funds should consist of Tier 1 Capital (Article 4(1)(118) Capital Requirements Regulation ("CRR")[284] – available via this link) as reflected in Article 25 and 26 of the Capital Requirements Regulation.

The role of virtual assets in this regard is yet unclear, especially in relation to applicable national accounting rules, which deviate between the various Member States on this topic. In any event, Article 36 CRR (deductibles from Tier 1 capital) should be taken into account in relation to virtual assets.

18.3. Crowdfunding and custody

Custody or safekeeping of financial instruments or crypto-assets on behalf of clients is regulated under MiFID II[285] and MiCAR[286], respectively. Under Article 10(3) ECSPR, a crowdfunding service provider cannot offer custodial services unless it holds a relevant MiFID II or MiCAR license.[287] If a service relates only to tokenized transferable securities, it might be covered by ECSPR and MiCAR is not relevant. If the service falls outside the scope of ECSPR, MiFID II will apply and it will be still outside the scope of MiCAR.

[284] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms.
[285] Article 4(1)(3) and Annex I (B) MiFID II.
[286] Article 3(17) MiCAR.
[287] See also Question 3.3 and Answer 3.3 of ESMA, 'Questions and Answers On the European crowdfunding service providers for business Regulation'.

The ECSPR appears not to require crowdfunding service providers to hold custody of issued securities or investor assets as the ECSPR appears to allow investors to self-custody their tokenised securities, which remains outside the ECSPR regulatory perimeter.

Platforms utilising blockchain-based infrastructure for investor transactions should ensure that their services in relation to tokenised securities remain within the scope of ECSPR's defined crowdfunding services and do not inadvertently trigger custodial obligations under MiFID II or MiCAR.

In addition, it is important to take into account possible national law custodial obligations in the individual Member States. Reference is made to recital (28) of the ECSPR and ESMA Q&A 801 cited below (*Italics* added):

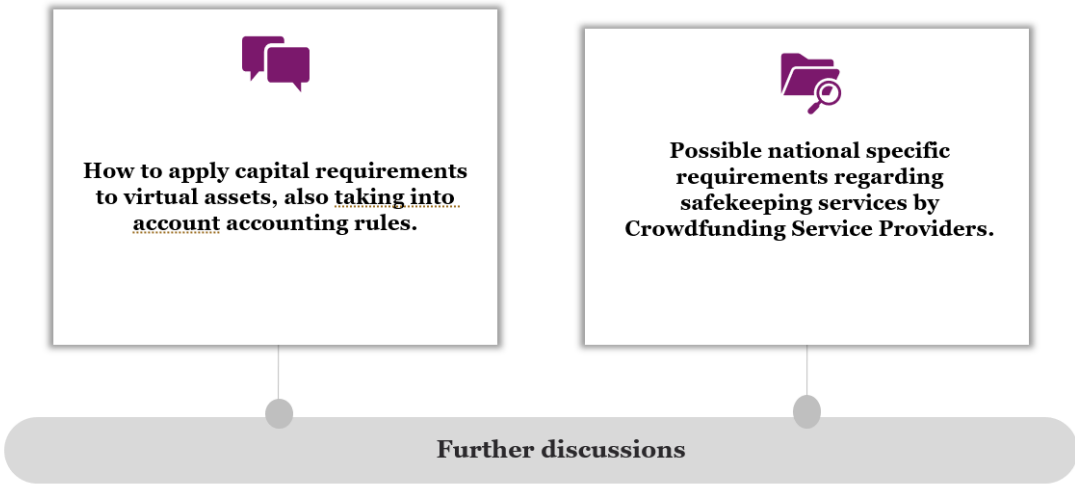
> **ECSPR recital (28):**
> "The requirements concerning safekeeping of assets are crucial for the protection of investors receiving crowdfunding services. Transferable securities or admitted instruments for crowdfunding purposes which can be registered in a financial instruments account or which can be physically delivered to the custodian should be safe-kept by a qualified custodian, which is authorised in accordance with Directive 2013/36/EU or 2014/65/EU. Depending on the type of assets to be safe-kept, assets are either to be held in custody, as with transferable securities which can be registered in a financial instruments account or which can be physically delivered, or to be subject to ownership verification and record-keeping. *Safekeeping of transferable securities or admitted instruments for crowdfunding purposes that in accordance with national law are only registered with the project owner or its agent, such as investments in non-listed companies*, or are held on an individually segregated account that a client could open directly with a central securities depository, *is considered equivalent to asset safekeeping by qualified custodians*."
>
> **ESMA Q&A (**ESMA_QA_801)
> "As indicated in Recital 28 of the ECSPR, the safekeeping of transferable securities or admitted instruments for crowdfunding purposes that, in accordance with national law, are only registered with the project owner or its agent or are held on an individually segregated account that a client could open directly with a central securities depository shall be considered equivalent to asset safekeeping by qualified custodians. *In such case, in accordance with Article 10(1) CSP shall clearly inform their clients about the safekeeping services according to national law*."

Further guidance or confirmation on EU level if it is correct to assume that the ECSPR does not require crowdfunding service providers to hold custody of issued securities or investor assets and to what extent the ECSPR allows for national specific requirements regarding safekeeping services by CSP's would be welcome.

18.4. Areas for further clarification & dialogue topics for the next cohort

Several areas for clarification or further discussion were identified:

- How to apply **capital requirements to virtual assets**, also taking into account accounting rules.
- Possible national specific requirements regarding **safekeeping services by Crowdfunding Service Providers**.


How to apply capital requirements to virtual assets, also taking into account accounting rules.
Possible national specific requirements regarding safekeeping services by Crowdfunding Service Providers.
Further discussions

19. Automated Market Makers & Liquidity Pools

19.1. Introduction Automated Market Makers

An Automated Market Maker (**"AMM"**) is a decentralized protocol that uses algorithmic formulas and smart contract based liquidity pools (**"LP"**), rather than traditional order books, to facilitate trading.

MiCAR allows AMM under certain conditions. Annex I of the Draft Transparency RTS supplementing MiCAR[288] identifies AMM as a contemplated trading system for the purposes of transparency requirements.

However, AMM is not considered in MiFID 2 and similar transparency provisions as in Annex I of the Draft Transparency RTS supplementing MiCAR are not available in connection with the DLT Pilot Regime[289].

Whether the AMM regulation under MiCAR is applicable will first of all be decided by the question if the crypto assets that are traded on the AMM qualify as financial instruments/securities.

19.2. Automated Market Makers for financial instruments

If the crypto assets that are traded through the AMM are financial instruments, MiCAR will not be applicable.

In this case the entity operating a trading venue on the basis of an AMM with LP could qualify as an MTF requiring a license under MiFID 2[290]/MiFIR[291]. In addition, a permission under the DLT Pilot Regime would be required (and consequently the entity operating the AMM would need to have legal personality).[292]

In addition, the tokenization of the financial instruments (securities) may under certain circumstances be regarded as an investment service (i.e. placing) which also incurs license obligations under MiFID 2.

The DLT Pilot Regime does not include a prohibition of operating a trading venue on the basis of an AMM. The AMM could be considered a DLT TSS under the DLT Pilot Regime if the criteria are met.

The transparency requirements (pre-trade, post-trade and transaction reporting) laid down in MiFIR would have to be complied with and how these requirements will be met will likely be a relevant consideration during the application process.

---

[288] Draft Commission Delegated Regulation (EU) …/... of 28.11.2024 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the manner in which crypto-asset service providers operating a trading platform ("**Draft Transparency RTS**").

[289] Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU ("**DLT Pilot Regime**").

[290] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU ("**MiFID II**")

[291] Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 ("**MIFIR**")

[292] See in addition for example Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 ("**CSDR**") or Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers ("**AIFMD**").

- Pre-trade transparency requirements in relation to shares[293] include making information available to the public on a continuous basis during normal trading hours to allow investors and other market participants to assess dynamics and soundness of the market for any specific financial instrument traded on a trading venue.

- Post-trade transparency requirements in relation to shares[294] include making information available to the public on a continuous basis during normal trading hours to allow investors and other market participants to assess dynamics and soundness of the market for any specific financial instrument traded on a trading venue.

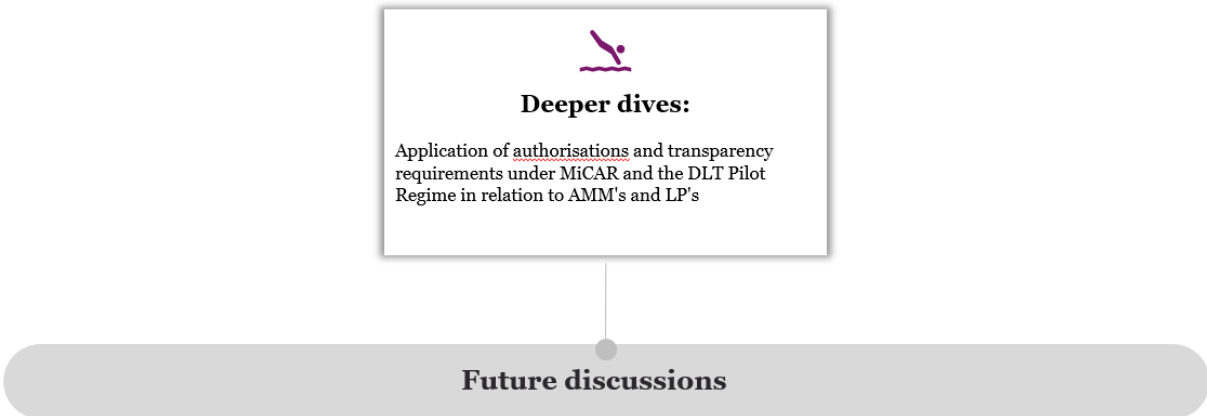
- Transaction Reporting Obligations in relation to shares are laid down in Article 26(1) of MiFIR which requires that all transactions in financial instruments, whether executed on a trading venue or not, must be reported to the competent authority. The reports must contain complete and accurate details of the transactions and be submitted as quickly as possible, and no later than the close of the following working day. This transaction reporting requirement ensures that national competent authorities (NCAs) can effectively monitor trading activity and behaviour within the scope of financial instruments covered under MiFID II. Exemption possible under DLT Pilot Regime if the conditions are met.

On the basis of MiFIR and the DLT Pilot regime, the possibility exists to apply for an exception of certain of these transparency requirements (the transaction reporting obligations) which could be granted by the national competent authority if the conditions of the DLT Pilot regime are met.

During the dialogues the question has come up how MiFIR pre- and post-trade transparency requirements should be applied to an AMM trading system under the DLT Pilot Regime and if the regulation of AMMs under MiCAR could provide a model for measures within the DLT Pilot Regime.

This would be an area where further guidance by ESMA would be welcome.[295]

The use of EMTs for settlement within an AMM Liquidity Pool appears not to require a separate license under MiCAR, if the operator holds a MiFID licence and the notification procedure under MiCAR is complied with.[296] Also in relation to this topic additional guidance from ESMA would be welcome.



[293] Articles 3 – 4 MiFIR.
[294] Articles 6-7 MiFIR
[295] Recital (54) DLT Pilot Regime.
[296] Article 60(3) MiCAR.

20. Conclusions and next steps

This 2nd cohort best practices report presents the best practices, lessons learned and recommendations that were identified during the 2nd round of dialogues for the European Blockchain Sandbox. The 2nd round of dialogues was able to build on the robust regulatory sandbox framework and the experiences and feedback gained during the 1st round of dialogues and the 1st cohort best practices report that was published in June 2024 (link).

The 2nd round of dialogues has again resulted in impressive and encouraging results with numerous best practices, lessons learned and recommendations at the intersection of innovation and many regulatory areas.

Feedback from the 2nd cohort of selected use cases and participating regulators/authorities is again very positive. The use cases appreciate the legal/regulatory guidance and the opportunity for open dialogue with regulators/authorities. The regulators/authorities appreciate the chance to learn more about DLT use cases (where relevant in combination with other innovative technologies) and to have a cross-border dialogue with other national and EU regulators/authorities. The adjustments in the format of the dialogues which were implemented as a result of the feedback from the 1st round of dialogues were welcomed by the participating regulators/authorities. These adjustments included, in particular, a change of the set-up of the blockchain expert meeting in the preparation of the dialogues (no longer on a per use case basis) and the introduction of a regulator-only meeting between the 1st and 2nd dialogue meeting for the financial sector dialogues, with many participating national competent authorities for each dialogue.

In its 2nd year of operation, the project has further matured. More regulatory areas and competent authorities were involved in the dialogues with even more engagement by participating national and EU regulators than in the 1st round as shown by the following key indicators:

- As for cohort 1, in the 2nd round all 20 selected use cases were matched with competent regulators/authorities and all dialogues resulted in best practices and lessons learned that could be used as building blocks for 2nd cohort best practices report.[297]
- On average 8 national/EU regulators per dialogue (compared to an average of 4 national/EU regulators in the 1st round and a minimum number of 1.5 regulators per dialogue in the tender specifications).
- Range of 2 – 15 national/EU regulators per dialogue (compared to a range of 1 – 8 national/EU regulators in the 1st round).
- Individual regulators participated in 1 to 8 use case dialogues (compared to a range of 1 to 4 in the 1st round).
- A combination of regulatory areas in 9 dialogues (compared to a combination of regulatory areas in 5 dialogues in the 1st round).
- The 2nd round of dialogues resulted in more concrete and extensive best practices and lessons learned compared to the 1st round of dialogues, involving even more regulatory areas and many more regulators (in total 85 participating regulators/authorities compared to over 50 in the 1st round).

After having succesfully completed two rounds of dialogues for the 2023 and 2024 cohorts of use cases, it is safe to say that the European Blockchain Sandbox is delivering a clear and positive impact to enhance legal/regulatory certainty for Blockchain/DLT solutions, often in

[297] One regulatory dialogue is still ongoing and will be completed in May 2025.

combination with other innovative technologies through an open and constructive regulatory dialogue between innovators and regulators. This important outcome has been achieved thanks to the following results:

- increased legal certainty through enhancing a better understanding of relevant laws and regulations by innovators and greater confidence of compliance;
- enhancing confidence among stakeholders and regulators/authorities by showing the potential of Blockchain/DLT solutions, in combination with other innovative technologies and/or regulatory instruments such as the eIDAS 2 regulation to support effective and efficient compliance and supervision across different industry sectors;
- the possibility to improve the regulatory framework as a result of the identification of regulatory issues and solutions and of areas for clarification, leading to more effective regulations;
- cross border collaboration facilitated by the project among European and national regulators/authorities and innovators, promoting a more unified regulatory approach of Blockchain/DLT solutions, where relevant in combination with other innovative technologies, which will enhance more harmonized regulatory practices and will help to create a more cohesive regulatory framework;
- facilitating the sharing of knowledge and experience between regulators/authorities and with innovators on the basis of concrete use cases resulting in a better understanding of compliance requirements among innovators and regulators/authorities;
- acceleration of innovation by providing a safe environment for refining innovative applications including Blockchain/DLT solutions to support compliance by design;

The EBS project team is looking forward to the 3rd cohort. Regulatory areas and topics for further discussion have been identified in the 2nd round and during the application and selection proces for the 3rd cohort. Important elements for the 3rd cohort will be, on the one hand an increased focus on a combination of innovative technologies such as DLT/Blockchain in combination with AI, IoT, Cloud computing, and on the other hand deeper dives on the basis of ongoing experiences in the Member States and new regulatory developments on EU level such as the expected blockchain guidelines by the EDPB, the implementing regulations for electronic ledgers on the basis of eIDAS 2 and expected further developments in the areas of auditing/certification of smart contracts, the development of standards including for the development and deployment of smart contracts and the implementation of the AI Act. In addition, the 3rd round of dialogues will provide the opportunity to discuss Blockchain/DLT solutions in additional industry sectors such as energy and health care.

Almost all 2nd cohort participating regulators/authorities are interested in participating again in the 3rd round of dialogues (depending on use cases and regulatory areas/topics) and the adjustments in the format of the dialogues in accordance with the feedback at the end of the 1st round of dialogues have worked out well. Therefore no major adjustments in the format of the dialogues are foreseen for the 3rd round of dialogues.

In concluding, the expectation is that the regulatory dialogues with the lessons learned from the 1st and the 2nd cohort can be further developed and deepened in the 3rd round, enhancing legal/regulatory certainty for innovators and regulators and enhancing trust and cooperation between innovators and regulators/authorities to ensure that regulation can increasingly become a catalystfor inovation.

The European Blockchain Sandbox project team would like to thank all participants in the 2nd round of dialogues for sharing their most valuable expertise, insights and experiences and for contributing to the best practices, lessons learned and recommendations that were identified during the dialogue meetings and are published in this best practices report.

Finally, the EBS project team would like to thank the project team at DG CONNECT for another year of seamless cooperation with excellent input and guidance that is provided at all stages of the project.

21. List of abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
AML	Anti money laundering
ARF	Architecture and Reference Framework
ASP	Application service provider
CASP	Crypto-assets service provider
CDD	Customer due diligence
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CO_2	Carbon dioxide
DAO	Depending on the context: Data Altruism Organisation (in the sense of the Data Governance Act) or Decentralized Autonomous Organization
DID	Decentralised Identity
DISP	Data Intermediation Service Provider
DLT	Distributed Ledger Technology
DP	Data Protection
DPP	Digital product passport
EAA	Electronic Attestation of Attributes
EBA	European Banking Authority
EBP	European Blockchain Partnership
EBS	European Blockchain Sandbox
EBSI	European Blockchain Services Infrastructure
EC	European Commission
ECJ	Court of Justice of the European Union
EDIC	European Digital Infrastructure Consortium
EDPB	European Data Protection Board
eFTI4EU	Electronic Freight Transport Information for Europe
eID	electronic Identification
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Cybersecurity
ESG	Environmental, Social and Governance
ESMA	European Securities and Markets Authority
ETSI	European Telecommunications Standards Institute
EU	European Union
EUDI	European Union Digital Identity
EU ETS	European Union Emissions Trading System
GDPR	General Data Protection Regulation
IoT	Internet of Things
IP	Intellectual Property
ISO	International Organization for Standardization
IT	Information Technology
KYC	Know Your Customer
Member States	EU/EEA Member States
MRV	Monitoring, reporting and verifying (based on the MRR & AVR)
MS	Member State(s)
MSP	Managed service provider

MSSP	Managed security services provider
NFT	Non-Fungible Token
PID	Person Identification Data
PUB_EAA	Public Body Authentic Source EAAs which are issued by or on behalf of a public body responsible for an authentic source
QEAA	Qualified Electronic Attestation of Attributes
QEL	Qualified Electronic Ledger
QTSP	Qualified Trust Service Provider
SCA	Strong Customer Authentication
SCE	Société Coopérative Européenne; European Cooperative Society
SPV	Special Purpose Vehicle
TSP	Trust service provider
UNTP	United Nations Transparency Protocol
VASP	Virtual Asset Service Provider
VAT	Value Added Tax

22. Terms and Definitions

22.1. Terms used in the Report

Term	Explanation
AI	Artificial Intelligence
AI System	A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[298]
Distributed ledger	An information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism.[299]
Distributed ledger address	An alphanumeric code that identifies an address on a network using distributed ledger technology (DLT) or similar technology where crypto-assets can be sent or received.[300]
'Distributed ledger technology' or 'DLT'	A technology that enables the operation and use of distributed ledgers.[301]
EBSI	European Blockchain Services Infrastructure.[302]
Electronic identification or eID	The process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person.[303]
Electronic identification means	A material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service.[304]
EUDI Wallet	European Digital Identity Wallet
European Digital Identity Wallet	An electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals.[305]

[298] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
[299] Article 2(2) DLT-pilot Regime and Article 3(1)(2) MiCA Regulation.
[300] Article 3(18) of Regulation 2023/1113 on information accompanying transfers of funds and certain crypto-assets.
[301] Article 2(1) DLT-Pilot Regime and Article 3(1)(1) MiCA Regulation
[302] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home
[303] Article 3(1) eIDAS 2 regulation.
[304] Article 3(2) eIDAS 2 regulation.

[305] Article 3(42) eIDAS 2

On-chain data	Any information that is stored directly on the blockchain.
Off-chain data	Any data that is stored outside of the blockchain but can interact with it when needed.
IoT	Internet of Things
Member State	A Member State of the EU/EEA
Regulators/Authorities	The regulator(s) and authorit(y)(ies) that participate together with the selected use case owners in the European Blockchain Sandbox.
SCE	Société Coopérative Européenne; European Cooperative Society
Smart contracts	A computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering.[306]
Trust services	List of trust services defined in the eIDAS 2 regulation.[307]

22.2. Common short forms of EU legislation

Short form	Full reference
AI Act	Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
AIFMD	Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010.
Amendment of the Company Directive	Directive (EU) 2025/25 of the European Parliament and of the Council of 19 December 2024 amending Directives 2009/102/EC and (EU) 2017/1132 as regards further expanding and upgrading the use of digital tools and processes in company law.
AMLD IV	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as most recently amended by Directive (EU) 2024/1226 of the European Parliament and of the Council of 24 April 2024 on the definition of criminal offences and penalties for the violation of Union restrictive measures.
AMLD V	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the

[306] Article 2(39) of the Data Act.
[307] Article 3(16) of the eIDAS 2 Regulation.

	prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU
AMLD VI	Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849
AMLR	Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
AVR	Commission Implementing Regulation (EU) 2018/2067 on the verification of data and on the accreditation of verifiers pursuant to Directive 2003/87/EC of the European Parliament and of the Council, lastly amended by Commission Implementing Regulation (EU) 2020/2084 of 14 December 2020.
Battery Regulation	Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries.
Commission Delegated Regulation (EU) 2023/2917	Commission Delegated Regulation (EU) 2023/2917 of 20 October 2023 on the verification activities, accreditation of verifiers and approval of monitoring plans by administering authorities.
Company Law Directive	Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law as most recently amended by Directive (EU 2025/25.
CSDR	Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (Central Securities Depository Regulation), lastly amended by Regulation (EU) 2022/858 (DLT Pilot Regulation).
CSRD	Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting.
EU Green Deal	Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting.
Data regulation	The Data Act, the Data Governance Act and the Digital Services Act
Data Act	Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data.
Data Governance Act	Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance.

Digital Company Law Directive	Directive (EU) 2019/1151 of the European Parliament and of the Council of 20 June 2019 amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law.
Directive (EU) 2023/959	Directive (EU) 2023/959 of the European Parliament and of the Council of 10 May 2023 amending Directive 2003/87/EC establishing a system for greenhouse gas emission allowance trading.
DLT-Pilot Regime	Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology.
DORA	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.
DSA (or Digital Services Act)	Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services.
ECSPR	Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937.
EEIG Regulation	Council Regulation (EEC) No 2137/85 of 25 July 1985 on the European Economic Interest Grouping (EEIG).
eIDAS 1	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.
eIDAS 2	Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
EMD II	Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions.
ESPR	Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC.
ESRS	Commission Delegated Regulation (EU) 2023/2772 of 31 July 2023 supplementing Directive 2013/34/EU of the European Parliament and of the Council as regards sustainability reporting standards (''ESRS'').
EUDR	Regulation (EU) 2023/1115 of the European Parliament and of the Council of 31 May 2023 on the making available on the Union market and the export from the Union of certain commodities and products associated with deforestation and forest degradation and repealing Regulation (EU) No 995/2010 ("EUDR").
EU ETS	Directive 2003/87/EC of the European Parliament and of the Council of 13 October 2003 establishing a system for greenhouse gas emission allowance trading, lastly amended by Directive (EU) 2023/959 of the European Parliament and of the Council of 10 May 2023.

EUI DPR	Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L119/1
Implementing Regulation of the UCC	Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of the Union Customs Code.
MiCAR	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.
MiFID II	Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.
MiFIR	Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/201, lastly amended by Regulation (EU) 2022/858 (DLT Pilot Regulation).
MRR	Commission Implementing Regulation (EU) 2018/2066 on the monitoring and reporting of greenhouse gas emissions pursuant to Directive 2003/87/EC of the European Parliament and of the Council, lastly amended by Commission Implementing Regulation (EU) 2023/2122 of 17 October 2023.
MRV Maritime Regulation	Regulation (EU) 2015/757 on the monitoring, reporting and verification of carbon dioxide emissions from maritime transport, as amended.
NIS2 (Directive)	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.
PRIIPs Regulation	Regulation (EU) No 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail and insurance-based investment products (PRIIPs).
Proposed Directive for ECBAs	Proposal of 5 September 2023 for a Directive of the European Parliament and of the Council on European cross-border associations (COM(2023) 516 final).
Prospectus Regulation	Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market.
PSD II	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.
RCE Directive	Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

Register Interconnection Regulation	Commission Implementing Regulation (EU) 2021/1042 of 18 June 2021 laying down rules for the application of Directive (EU) 2017/1132 of the European Parliament and of the Council as regards technical specifications and procedures for the system of interconnection of registers.
Sanctions lists	Consolidated list of persons, groups and entities subject to EU financial sanctions: data.europa.eu
SCE Regulation	Council Regulation (EC) No 1435/2003 of 22 July 2003 on the Statute for a European Cooperative Society (SCE).
SE Regulation	Council Regulation (EC) No 2157/2001 of 8 October 2001 on the Statute for a European company (SE)
Shareholders Rights Directive	Directive 2007/36/EC of the European Parliament and of the Council of 11 July 2007 on the exercise of certain rights of shareholders in listed companies.
TFR	Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849.
UNESCO Convention 1970	UNESCO Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property (1970).
UCC	Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code. The European Commission has published a proposal to renew this regulation: EU Customs Reform: A data-driven vision for a simpler, smarter and safer Customs Union, 17 May 2023, which can be accessed via the following hyperlink: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2643.

23. Annexes

23.1. Use cases 2nd Cohort

Reference is made to the use case descriptions on the project website (available via: https://blockchain-observatory.ec.europa.eu/system/files/2025-04/2nd-cohort-best-practices-report). The use case descriptions are not part of the best practices report.

23.2. Annex to Chapter 5 (AI Act) – Overview of legal obligations to offering* AI Systems, tools, services, components, or processes (jointly referred to as "AI products") that are provided "under free and open source licences"

Legend:
Green: area where legal obligations are applicable.
Red: area where legal obligations are not applicable.
White: area where legal obligations could be applicable, depending on the exact circumstances.
Yellow: area where further clarification would be welcome.
Text: Elements that might change if the AI product is not offered under a free and open-source licence.

	Application of legal obligations to offering* AI products "Under free and open-source licence"				
		Applicability AI Act obligations (other than Art. 25)?	Applicability Art. 25(4) AI Act re. AI value chain supplier relationships	Contractual obligations?	Non-contractual liability/regulatory obligations in other national or EU legislation
1	To providers of High-Risk AI Systems (incl. Art. 25(1))	Yes (Art. 2(12) not applicable).	Yes, if making use of a supplied third-party product/service, except if the supplied product/service (including AI Systems?) qualify as open source as meant in the last sentence of Art. 25(4).	No	TBC***
2	To parties becoming High-Risk AI System provider under Art. 25(1)	Yes (Art. 2(12) not applicable).	Yes (in scope under Art. 25(4) jo. 25(1)), if making use of a supplied third-party product/service, except if the supplied product/service (including AI Systems?) qualify as open source as meant in the last sentence of Art. 25(4).	No	TBC***
3	To providers of other AI Systems	No (Exception Art. 2(12) applicable).	No (not in scope under Art. 25(4)).	No	TBC***
4	To third-party suppliers of tools, services, components, or processes that are used or integrated in a high-risk AI system	Not in scope under Art. 2(1).	Third-party supplier not the addressed party in Art. 25(4) (in view of Art. 2(1))? Art. 25(4) obligations including open-source exemption only addressed to the high-risk AI system provider?	No	TBC***
5	To third-party suppliers of AI systems that are used or integrated in a high-risk AI system	See the first three rows for the applicable color, as these third-party suppliers will also be providers of AI systems.	Third-party supplier not the addressed party in Art. 25(4) (in view of Art. 2(1))? Art. 25(4) obligations including open-source exemption only addressed to the high-risk AI system provider? Art. 25(4) open-source exemption also relevant for third-party suppliers of AI systems?	No	TBC***
6	To third-party suppliers of tools, services, components, or processes that are used or integrated in other AI systems	Not in scope under Art. 2(1).	Art. 25(4) not applicable to AI systems other than high-risk AI systems. Therefore, other scope-related questions in relation to Art. 25(4) not relevant.	No	TBC***

* NB: there are other parties which may be regulated (deployers, importers and distributors). Notwithstanding, this table focuses on parties directly offering AI(-related) products/services under own name/trademark.

** Assuming that a contract has been concluded. This will generally be the case, considering that the product/service in question is offered against a price or other monetary compensation.

*** Depending on further analysis. The AILD is listed for withdrawal in the EC's 2025 work programme.

23.3. Annex to Chapter 6 (DAO's) - Case study - Can DAO characteristics be facilitated by an SCE?

The overview below includes initial observations for further discussion, taking into account legal/regulatory developments in the area of legal entities/partnerships on EU and national level.

These observations will need to be tested for each individual DAO on the basis of its characteristics such as profit / non-profit, legal wrapper or not, purpose/activities (regulated or not), internal organization and on the basis of applicable national legislation.

	Legal requirements in the SCE Regulation (1435/2003)	Possible issues and solutions if applied in a DAO context
1.	**Formation of an SCE** Art. 2 SCE Regulation: by five or more natural (or legal) persons resident in at least two Member States. Art. 12 SCE Regulation: Publication of documents in the Member States Art. 17 SCE Regulation: formation governed by the law applicable to cooperatives in the MS in which the SCE establishes its registered office. UBO registration is mandatory in every Member State for all corporate and other legal entities and trusts in accordance with the national implementations of the AML Directive (EU) 2015/849 as amended on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (article 30 for legal entities, article 31 for trusts).	➢ Incorporation requirements for SCE's are determined by national law in the country of incorporation, including corporate bodies and UBO and other incorporation formalities ➢ Registration and publication requirements are determined by the applicable national registration requirements which may include different registration requirements and registration requirements in more Member States depending on national requirements. ➢ A DAO which intends to structure itself through an SCE will need to determine the country of incorporation depending on the characteristics/needs of the DAO. ➢ Reference is made to the DAO Study: Annex VIII – Table 16: Legal Frameworks Governing Cooperatives Across the EU27 ➢ Examples: o NL: Notarial deed, Registration in UBO register; Registration in commercial register; UBO criteria on the basis of the AML Directive (more than 25%). If no DAO member has more than 25%, every board member should be registered as UBO unless there are vote members with special voting powers o ES: incorporation requires a notarial deed; registration with the commercial register and with the UBO register; UBO criteria: If no DAO member has more than 25%: every board member.
2.	**Well defined purpose which is aligned with the interest of the DAO members** Article 1 SCE Regulation (cooperative society) Article 5 SCE Regulation (Statutes)	➢ The well-defined purpose of both SCEs and DAOs seems compatible, assuming the governance rules (statutes) of the SCE can accommodate the specific mechanics of DAOs, such as smart contract-based decision-making.
3.	**Physical address** Article 5(4) and 6 SCE Regulation: An SCE requires an address of the registered office to be included in the statutes, which is located in the same Member State as its 'head office'	➢ Incorporation of an SCE requires a physical address in the sense of Article 5(4) and 6 SCE. ➢ Although this is not in line with the characteristics of most DAO's without a legal wrapper, the lack of a physical address may also cause issues from a regulatory compliance perspective depending on the activities of the DAO. EU regulation often requires a physical address for communication purposes as well. (Chapter 5, under c, Best Practices report 1st round of EBS dialogues). ➢ A mere "legal representative" will likely not be enough in view of Article 5(4) SCE Regulation. However, it is not uncommon for companies with a flexible work force to choose a physical registered office; it does not need to be a 10 storey building;

	Article 7 SCE Regulation: transfer of registered office Article 12 SCE Regulation (Publication of docs in the Member States) Article 13 SCE Regulation (Notice in the OJ of the EU)	➢ A structure with an "Umbrella DAO" facilitating "Sub DAO's" might be useful to explore. But it is important to keep the business case of the DAO in mind: "the legal/regulatory analyses and where a DAO does dock in the real world will be tailormade on the basis of the nature of the DAO activities and if these activities are regulated." ➢ Transfer of registered office of an SCE from one Member State to another requires that the SCE meets the national requirements of the Member State to which its office is transferred (which in practice requires dissolution and incorporating a new SCE)
4.	**Formalities in connection with shares; can shares in an SCE be tokenized?** Article 1(2) SCE Regulation: the subscribed capital of an SCE shall be divided into shares Article 3 SCE Regulation (minimum capital requirement): Minimum EUR 30,000 Article 4(1) SCE Regulation: The subscribed capital of an SCE shall be represented by the members' shares, expressed in the national currency. Article 4(2) SCE Regulation: The capital may be formed only of assets capable of economic assessment. Members' shares may not be issued for an undertaking to perform work or supply services. Article 4(3) SCE Regulation: Shares shall be held by named persons. Article 14(4) SCE Regulation: An alphabetical index of all members shall be kept at the registered office of the SCE, showing their addresses and the number and class, if appropriate, of the shares they hold. Any party having a direct legitimate interest may inspect the index on request and may obtain a copy of the whole or any part at a price not exceeding the administrative cost thereof.	➢ The shares in a SCE should be registered in the name of certain (natural or legal) persons who therefore should be known. This does not necessarily imply the need for a share register in physical format (examples: NL and ES). Requirements are determined by applicable national law. ➢ Based on Art. 4(2) SCE Regulation the minimum capital needs an *"economic assessment"*. There could, however, be a parallel structure of governance tokens in the DAO with different rights: economic tokens, contributing to the share capital, which are linked to shares, and governance tokens, which may not be linked to shares. Only the economic tokens that are linked to the shares in the SCE can be taken into account for the incorporation process. ➢ The minimum share capital (Art. 3 SCE Regulation) needs to be contributed by the shareholder members (holders of the economic tokens. This requirement does not mean that all shareholder members need to contribute equal amounts to the share capital. One or more shareholder members could pay more than others and the other shareholder members can contribute a nominal value (minimum 1 Euro). ➢ Can SCE shares be tokenized? No contra-indication in the SCE regulation but this also depends on national legislation and requires further analyses. If the SCE shares cannot be tokenized this could possibly be solved with the aforementioned parallel structure of tokens.
5.	**Distributed/multi stakeholder and transparent governance and interests (financial or non-financial). Is it possible to use smart contracts for decision-making?** Article 4 SCE Regulation: Capital of the SCE Article 5 SCE Regulation: Statutes	➢ The SCE Regulation does not seem to prohibit the use of smart contracts for engagement by and interaction with DAO members. ➢ The term "smart contract" is causing confusion. A smart contract can be merely a software code implementing agreements or implementing formal decisions. However, in DAO's there may be no other agreements or decisions but only smart contracts, meaning that the smart contracts also embody the contract or decision in a legal sense. ➢ An analysis of applicable national law is important as the focus of the SCE Regulation is on the establishment of an SCE and less on the operational phase. ➢ If the shares in the SCE can be tokenized, the use of smart contracts would not be a problem, and to the extent the shares cannot be tokenized or if governance tokens that are not linked to SCE-shares are used, a parallel structure as mentioned in the previous point could be used. The most important question is if the governance process in the SCE can be matched with the governance process in the DAO. In companies you see voting agreements in the Share Holders Agreement which are not included in the governance of the company laid down in the statutes. There appears to be an option to work with a similar parallel set-up using smart contracts in a DAO.
6.	**Required organs, including appointments and change of members; internal decision making and external representation**	➢ The SCE regulation requires certain corporate bodies as a minimum: a general meeting of shareholders and a management board (a supervisory organ is optional). ➢ This basic organizational structure can be a challenge for DAO's, as there is normally not a centralized decision- making body (management board). Governance decisions in a DAO are made based on tokens.

	Article 36 SCE Regulation: A general meeting is required next to either a supervisory organ and a management organ (two-tier system) or an administrative organ (one-tier system). Article 27 SCE Regulation: Members of the management board are appointed by the supervisory organ (two-tier) or by the general meeting (one-tier). Article 14 SCE Regulation (Acquisition of Membership): Acquisition of membership of an SCE shall be subject to the approval of the management or administrative organ	➢ Complete overlap of the general meeting and the management organ is an option on paper, but it would mean that all shareholders/members of the management board would have to be registered as UBOs and would be liable for mismanagement in accordance with national legislation. This is a less stringent liability compared to a situation without a legal wrapper, but still the question remains which members are prepared to take on this burden which is add odds with the assumption of equality of members in a DAO. ➢ A distinction should be made between the internal decision making and the external representation. The management board needs to be part of the internal organization in an SCE and shall represent the SCE (art. 37(1) SCE Regulation), but the representative function could further be established by the management board outside the DAO. ➢ However, the external representation does not solve the issue that the management board will be responsible for the internal organization/decision making and the members will need to be registered in the public registers (including the UBO register) and will be liable for mismanagement in accordance with national law. ➢ These challenges appear, however, not specifically linked to the SCE. The basic structure of legal entities is that they have a management board. Partnerships have partners and no management board, but in partnerships the members will be personally liable without the protection of a legal entity. ➢ If it is possible to have an external entity that could function as a management board and is entrusted with external representation, that could solve the problem for the SCE (or another legal wrapper). This is worth looking into. The management board can be external and although the management board is appointed by the members (or by the supervisory organ) it is not required that members of the management board are also members of the SCE. ➢ However, the aforementioned option does not yet accommodate the basic feature of the DAO that management decisions are jointly taken by the members/token holders and not by a management board (with approval of certain decisions by the members). ➢ Going forward, a completely new legal entity/structure could possibly be designed that accommodates the basic features of a DAO including that decisions are jointly taken by the members/token holders while the external representation and associated liability for mismanagement are not resting upon the individual DAO members. This external entity should not be an empty shell and provide financial recourse in the event of mismanagement.
7.	**Book-keeping and administration** No such requirements follow from the SCE Regulation. The focus of the SCE Regulation is more on the establishment of an SCE and less on the operational phase.	➢ Decentralised/electronic book-keeping and administration are not inconsistent with the SCE Regulation. ➢ Although decentralized/electronic bookkeeping and administration is not restricted in specific provisions in the SCE Regulation, there needs to be financial accountability which is governed by the legal provisions in the Member State where the SCE has its registered office (Chapter VI of the SCE Regulation) and the question is if decentralized/electronic decision making, bookkeeping and administration will be accepted under these national rules. ➢ Therefore, although decentralized/electronic bookkeeping and administration is not prohibited in the SCE Regulation of 2003 it is also not solved by this regulation and the possibilities will depend on national legislation/analyses in the individual Member States.
8.	**Connection between founders and co-ownership (limitation of liability of founders/individual members)** Article 1(2) SCE Regulation: Unless the statutes provide otherwise, no member shall be liable for more than the amount he, she or it has subscribed for.	➢ A legal (SCE) wrapper will not provide a 100% shield against liability claims (in the event of mismanagement) and regulatory requirements will need to be complied with, but it will provide more certainty for individual members compared to a DAO without a legal wrapper. ➢ Liability will be an important part of the dialogue following the publication of the DAO Study. On the one hand liability cannot be fully excluded, but it should be possible to protect individual DAO members against unlimited liability. This issue is linked to the question about the liability of members of the management board in a legal entity (reference made to point 6).

	Article 51 SCE Regulation (Civil liability): Members of management, supervisory and administrative organs shall be liable, in accordance with the provisions applicable to cooperatives in the Member State in which the SCE's registered office is situated, for loss or damage sustained by the SCE following any breach on their part of the legal, statutory or other obligations inherent in their duties	
9.	Rules for winding up a DAO Winding-up is provided for in Articles 72 – 76 of the SCE Regulation, provided that the law of the Member State in which the registered office is situated applies.	➢ This requirement does not appear to raise specific issues in relation to DAO's.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centers. You can find the address of the center nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information center (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

KK-01-25-034-EN-N

Publications Office
of the European Union

doi: 10.2759/8586422
ISBN 978-92-68-26348-8