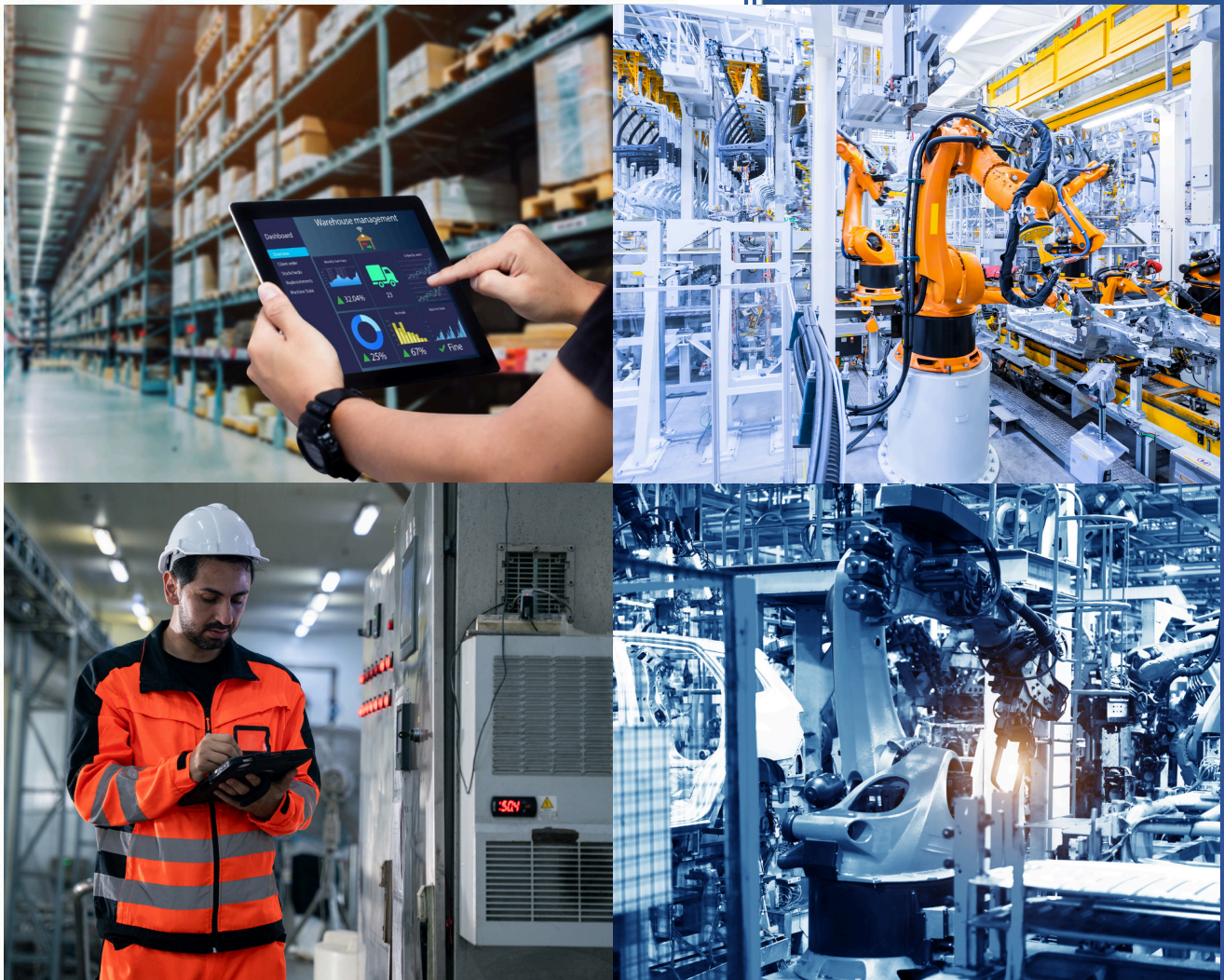# MASTT2040 Recommendations

Lead Authors: Anna Pająk and Krzysztof Pietrusewicz

Contributors: Haydn Thompson, Pieter Kesteloot, MASTT2040 Project

15/12/2025

MANUFACTURING AS A SERVICE FOR THE EU'S TWIN TRANSITION UNTIL 2040

Recommendations for Industrial Data Standardisation in Manufacturing for future Manufacturing as a Service

Document Control Page			
WP number	WP4		
Author(s)	Anna Pająk, Krzysztof Pietrusewicz (Polish Agency for Enterprise Development – PARP)		
Contributions	Haydn Thompson (Thhink), Pieter Kesteloot (Sirris)		
Type	R = Report		
Version	**Date**	**Authors**	**Partner Name**
V1	4/12/2025	Anna Pająk, Krzysztof Pietrusewicz	PARP
V2	8/12/2025	Anna Pająk, Krzysztof Pietrusewicz	PARP
Dissemination level	☐CO (Confidential, only for members of the consortium and Commission Services) ☒PU (Public)		
Requested deadline	31/12/2025		

Table of Contents

List of Figures

Executive Summary

This document presents recommendations derived from the analytical work conducted in the MASTT2040 project with respect to the role of data and its standardisation for future Manufacturing-as-a-Service business models. These recommendations are designed to guide the European Commission in formation of future policy actions and in promoting industrial data standardisation in support of European Industry. The work has considered visions for the future of Manufacturing-as-a-Service going to 2040 addressing key European goals with respect to resilience in supply chains, sustainability, circularity and how workers will utilise and integrate with technology in the future. A number of key strategic areas were identified for where action is needed. This includes:

- Trusted Data Spaces enabling safe and effective cooperation within Manufacturing-as-a-Service ecosystem,
- Interoperability based on data standardisation and digital tools,
- Circular Economy enabled MaaS,
- Regulation,
- Skills and Competences.

Under each area detailed specific actions are identified with respect to the development of supporting standards as well as funding initiatives to encourage the uptake of standards within industry at all levels from SMEs to large industry.

These actions provide a basis for strategic uptake via the European Commission Directorates and Agencies, Standardisation Development Organisations, Industry and SME Associations and European Digital Innovation Hubs as well as Legal, Contract and Ethics Platforms. Many stakeholders from these groups have been engaged via workshops, meetings and via circulation of MASTT2040 outcomes in the development of these recommendations and strategic actions.

There are, however, structural challenges within the European standardisation ecosystem which also need addressing in order to facilitate the adoption of these actions. MASTT2040 advocates that a coordinated approach is adopted to address the current high degree of fragmentation in data standardisation activities, with the need to facilitate targeted actions to avoid duplication of effort, and to ensure that the solutions developed take into account the perspectives of all stakeholders. This needs to particularly consider how the proposed solutions may impact European manufacturing stakeholders from large industry to SMEs in individual economic sectors and countries with varying levels of digital maturity.

1. Introduction

The MASTT2040 project applies **participatory strategic foresight** to anticipate changes, opportunities, and disruptions that will shape Manufacturing-as-a-Service up to 2040. By engaging a broad range of stakeholders, the approach builds a shared vision, roadmap and recommendations that guide decision-making and actions, aiming to advance Europe's industrial manufacturing resilience, digitalisation, circularity, decarbonisation, and sustainability.

The results of analytical work conducted in the MASTT2040 project with respect to the role of data and its standardisation in the wider adoption of Manufacturing-as-a-Service business models in Europe is presented. The ultimate goal guiding the work was to provide recommendations for the European Commission in the area of industrial data standardisation and related policies.

The recommendations are supposed to highlight the need for new standardisation activities in relation to the identified standardisation needs of future MaaS approaches, towards the Rolling Plan for standardisation[1] which is a document that is reviewed each year based on input from the Commission and advice from the European multi-stakeholder platform on ICT standardisation (MSP).

The document firstly highlights the methodology adopted and then presents the recommendations clustered into five key areas. These are:

- Trusted Data Spaces,
- Interoperability,
- Circular Economy,
- Regulations,
- Skills and Competences.

For each of the key area's recommendations are described in the following way:

- An overview on the area and its scope,
- A list of recommended action domains, for each action domain a list of actions,
- The actions grouped by category, relevant to possible groups of Stakeholders ([1] financing, pilot projects and infrastructure development; [2] standardisation in the area of data, cloud aspects and cybersecurity; [3] data management, legal compliance, regulations; [4] organisational security and certification; [5] Competences, skills, capacity building and knowledge dissemination; [6] Support for SMEs, support tools and direct assistance).

Manufacturing-as-a-Service is a functional combination of four seemingly independent business models characteristic of a modern manufacturing company. 'Distributed on-demand manufacturing of parts and components' is the basis for modern production tailored to customer needs and expectations, regardless of whether the order is for a large or small series. 'Custom design automation and access to digital product models contributes to shortening the design of products, which are then manufactured on demand, thanks to digitisation, automation available in design tools, and the use of digital twin technologies. 'Provision and servitisation of production equipment' supports modern

---

[1] https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation

personalised on-demand production in terms of ensuring continuity of operation in a modern business model as well as flexibility of infrastructure availability. 'Enabling the Circular Economy' completes the picture of MaaS by supporting compliance with the Circular Economy/ Green Deal on the one hand, and on the other hand by integrating the environmental aspects of on-demand production throughout the value chain.

Business value	Distributed on-demand manufacturing of parts and components
What it shares	Manufacturing capacity, data, logistics, **standards**
Payment model	Pay-per-use or per-order transaction-based
Supplier's responsibilities	Provide capacity, **quality**, data, **traceability**
What the client gets	Fast, scalable, transparent, cost-optimized, **sustainable** manufacturing services

Business value	Enabling the Circular Economy
What it shares	Recycled materials, R-cycle services, **sustainability** data, **DPPs**
Payment model	Pay-per-service, subscription, outcome-based, certification/licensing fees
Supplier's responsibilities	Ensure transparency, deliver circular services, comply with regulations, maintain certification
What the client gets	Sustainable products, cost/ resource efficiency, **compliance** and competitive advantage
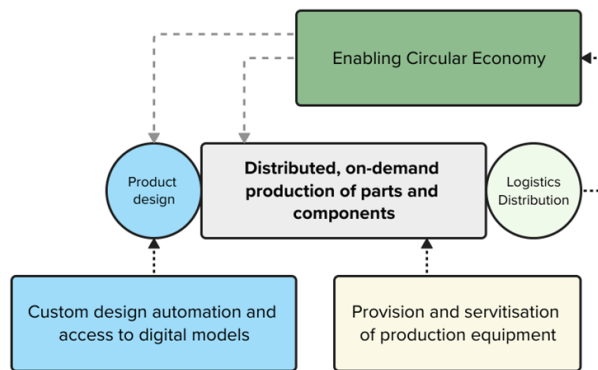
Manufacturing-as-a-Service is a distributed system of production in which **resources are offered as a services** (including data and software), allowing manufacturers to **access distributed providers** to implement their manufacturing processes

Business value	Custom design automation and access to digital product models
What it shares	**Digital product models**, automated design tools, **standards** and simulations
Payment model	Pay-per-design, subscription, licensing, sometimes bundled with production
Supplier's responsibilities	Provide models, automation, **IP protection**, **interoperability**
What the client gets	Faster, cheaper, customizable, validated designs linked to distributed MaaS production

Business value	Provision and servitisation of production equipment
What it shares	Equipment, infrastructure, cloud services, **operational data**
Payment model	Pay-per-use, subscription or outcome-based
Supplier's responsibilities	Maintain and optimize equipment, **ensure interoperability**, provide lifecycle services
What the client gets	Flexible access, cost savings, performance optimization, scalability and sustainability

Figure 1. Future manufacturing business models integration within MaaS

When analysing areas of standardisation, developing recommendations and proposing actions to increase the momentum of MaaS implementation in Europe, all these models must be taken into account simultaneously. This makes it difficult to conduct any kind of analysis.

The following chapters discuss how a series of recommendations was methodically developed.

2. Methodology overview

The work carried out in the MASTT2040 foresight project was based on extensive literature analysis and market analyses, including best practices and interviews with companies implementing MaaS models in Europe. Strategic foresight methods were applied providing extensive and comprehensive study including trend analysis, Delphi survey, scenario method and strategic roadmapping. All activities undertaken in the project ensured the active involvement of a wide range of stakeholders of the manufacturing sector in Europe. For a detailed understanding of the intermediate results of the various stages of the project and the research work undertaken, relevant publications from the MASTT2040 project are available at https://www.mastt2040.eu/
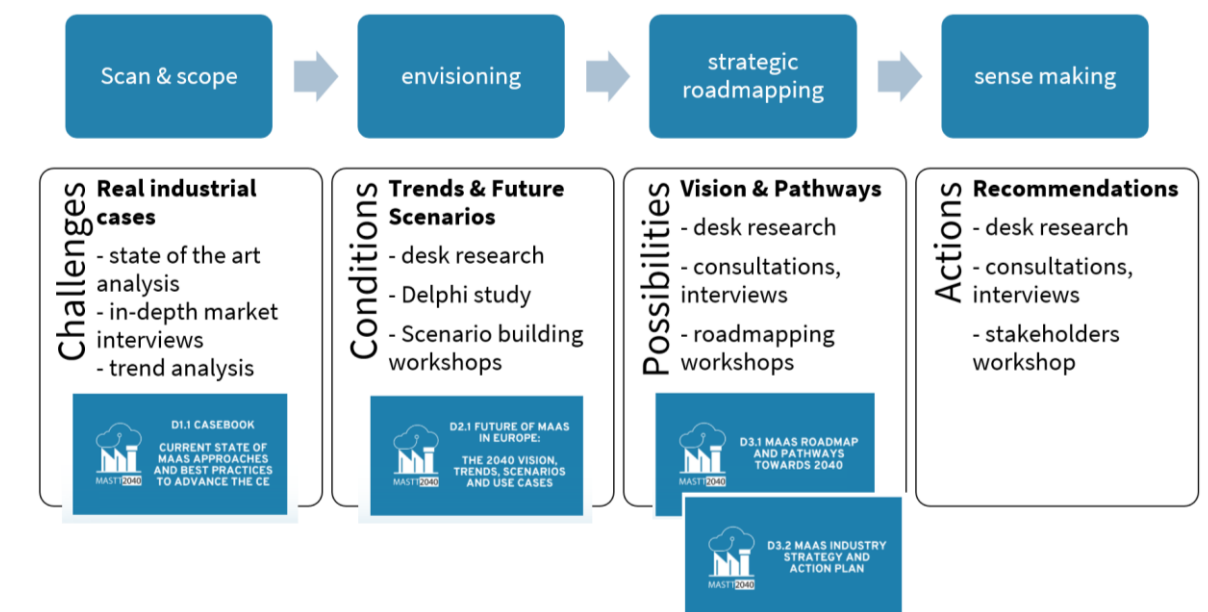
Figure 2. Research methods applied in MASTT2040 project

2.1. Lessons learned with respect to standardisation and regulation

The first phase of the study (scan & scope) defined the foresight framework by setting the scope, objectives, audience, and key stakeholders of MASTT2040. Using desk research and structured interviews, it mapped the current state of MaaS in European manufacturing, its links to the circular economy and resilience strategies, and its alignment with EU policy goals. This phase identified the defining features of MaaS, relevant use cases, and major forces shaping Europe's manufacturing.

*A central finding was that existing MaaS solutions are limited by proprietary systems, restricting openness, interoperability, and scalability. To unlock MaaS full potential, **open systems and shared standards are needed** to ensure cross-platform interoperability, support collaborative value networks, and build a resilient, future-proof manufacturing ecosystem.*

The second stage (envisioning) developed scenarios for EU manufacturing in 2040, exploring how distributed MaaS and centralised models interact under key trends such as digitisation, decarbonisation, circularity, and sustainability.

*These scenarios showed MaaS evolving into a cross-border ecosystem that depends on interoperability, trust, and **alignment across data spaces and regulations**.*

*This phase highlighted **standardisation as a critical enabler**[2] – ensuring platform compatibility, secure data exchange, and governance frameworks needed for scalable, reliable, and sustainable **MaaS networks across Europe**.*

The third stage (strategic roadmap) transformed the scenarios into actionable pathways for MaaS development to 2040, defining short-, medium-, and long-term strategies for resilience, sustainability, and human-centric production. Through collaborative roadmapping workshops, an Industry Strategy and Action Plan was also produced aligned with EU goals for circularity, decarbonisation, and competitiveness. This identified key strategic areas where standardisation is required.

*The roadmap emphasised that MaaS can scale at the European level through open, interoperable systems underpinned by common standards – covering trusted data spaces, digital product passports, and cross-border interoperability frameworks. **Standardisation thus emerges as a core enabler** of the MaaS transformation, ensuring seamless, secure, and sustainable collaboration across industries in line with Europe's twin transition objectives.*

The fourth stage (sense-making and recommendations) assessed the previous results against existing regulations to guide Standards Development Organisations (SDOs) in prioritising MaaS-related standardisation. It introduced a framework for data standardisation needs in MaaS to identify **standardisation gaps**[3] in interoperability, cybersecurity, data spaces, and national data policies. Based on this, short-, medium-, and long-term actions are proposed to define the standards and data frameworks needed for MaaS ecosystems up to 2040. These recommendations, co-created with stakeholders, aim to steer strategic investments and remove barriers[4] to scalable, secure, and sustainable MaaS adoption across Europe.

2.2. Framework for standardisation needs in MaaS

The framework for data standardisation needs for MaaS adoption developed on the project results is presented on Fig. 2

---

[2] **Enabler** (force pushing standardisation forward – regulation, policy, industry demand, digitalisation) or driver in MaaS standardisation: an external force or supportive mechanism (policy, regulation, market demand, industry initiative or technology trend) that pushes or accelerates the need for standardisation.

[3] **A standardisation gap** (what's missing – new standards required) in MaaS is a critical missing element in interoperability, governance or capability that prevents MaaS ecosystems from scaling, being trusted or contributing to the EU's TWIN transition. Gaps arise when existing standards do not sufficiently address data, processes or business models, making it hard for MaaS actors (suppliers, platforms, clients, regulators) to collaborate seamlessly. A standardisation gap in MaaS is an area where the lack of harmonised technical, data, or governance standards prevent MaaS ecosystems from ensuring interoperability, trust, scalability, sustainability and alignment with EU twin transition goals.

[4] **Barriers in MaaS standardisation** are practical obstacles that prevent or slow down the implementation, adoption or scaling of MaaS ecosystems, even when some standards already exist. Barriers often arise from fragmentation, lack of alignment, inconsistent adoption or conflicting regulations/market practices.
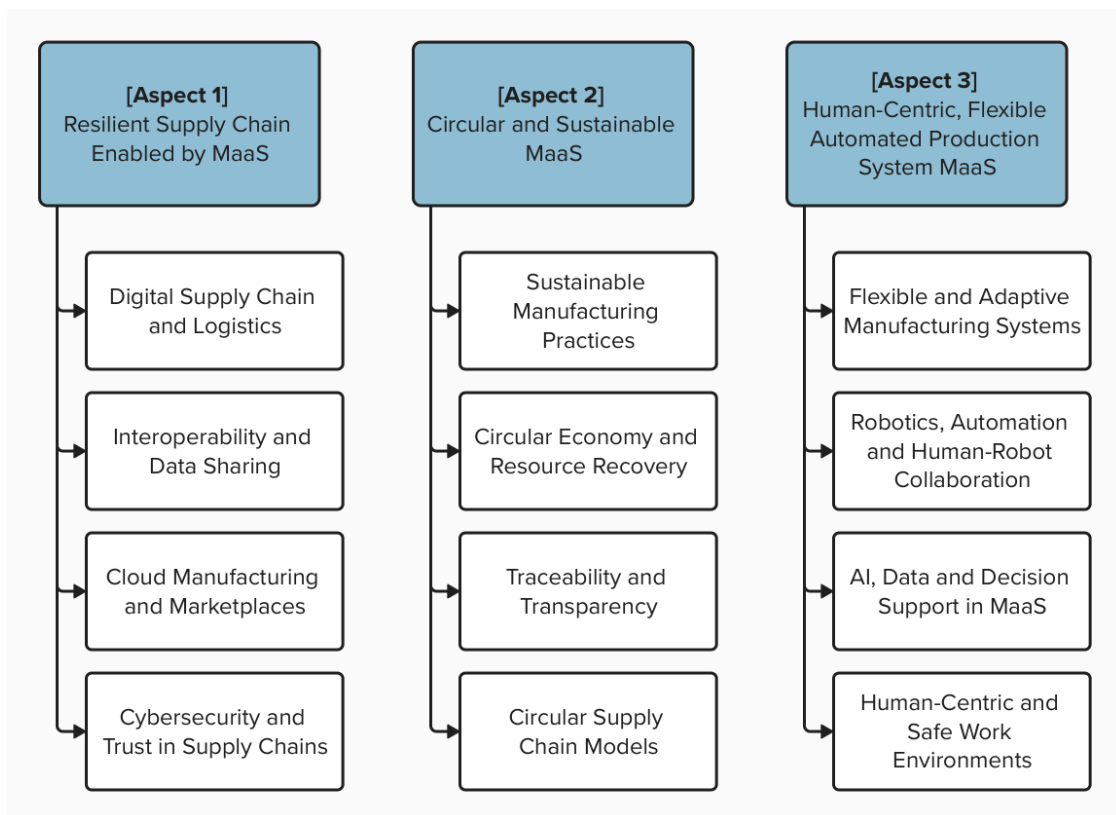
Figure 3. MASTT2040 Framework for data standardisation needs in MaaS

Key cross-cutting factors in the area of data standardisation in MaaS have also been identified (Fig. 3). The generic nature of most aspects relating to data standardisation is noteworthy.
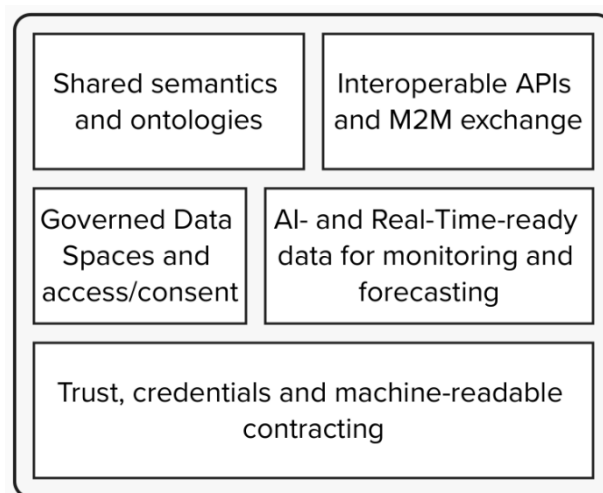

Figure 4. Data standardisation needs for MaaS cross-cutting factors

3. Recommendations for the future of MaaS

The stages of the study focused on the recommendations development comprised:

- **integration, validation and refinement of the MASTT2040 project findings** (including best practices and use cases, future scenarios and roadmaps) in order to **provide a picture of the data and the ecosystem solutions that MaaS enterprises will need to conduct their business** (up to 2040)
- **identification of existing ongoing standardisation activities** which meet the needs of future MaaS approaches or whether changes to existing activities as identified in the Rolling Plan for ICT Standardisation[5] or new standardisation efforts will be necessary
- **analysis of the current contributions in standardisation area and most important gaps** within the ongoing data standardisation efforts and current policies including specific issues such as cybersecurity, national data management policies and data spaces
- **formulation of recommendations regarding data standardisation** to support the achievement of the strategic objectives of European industrial policies and collaboration in future manufacturing ecosystems.
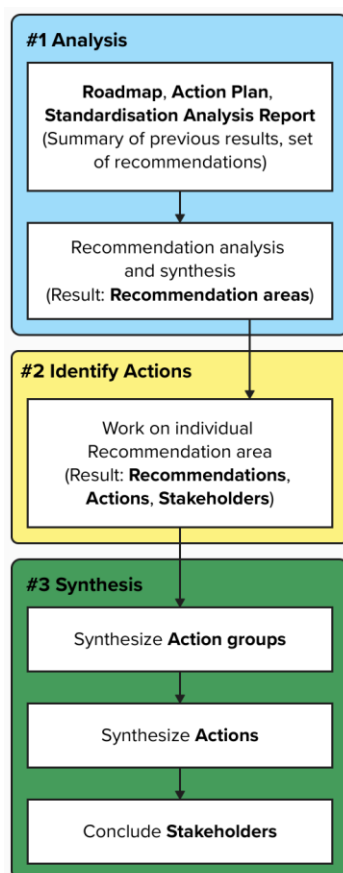
#1. Summary and analysis of recommendations contained in the results of the MASTT2040 project to date in the context of their relevance from the perspective of data standardisation policies.

#2. Clustering of the recommendations into five key areas according to identified themes considered most relevant from the perspective of standardisation policies: Trusted Data Spaces; Interoperability; Circular Economy; Regulations, Skills and Competences.

#3. Drafting of the recommendations including Recommended **Actions** were defined, potential **Stakeholders** to whom the **Recommendation** should be addressed were identified.

Action groups: [1] financing, pilot projects and infrastructure development; [2] standardisation in the area of data, cloud aspects and cybersecurity; [3] data management, legal compliance, regulations; [4] organisational security and certification; [5] Competences, skills, capacity building and knowledge dissemination; [6] Support for SMEs, support tools and direct assistance.

Figure 5. MASTT2040 recommendations development workflow and structure

---

3.1. Trusted Data Spaces enabling safe and effective cooperation within Manufacturing-as-a-Service ecosystem

In future, open MaaS ecosystem companies open their boundaries, digitally and operationally, to co-create, co-deliver and co-evolve with partners

3.1.1. Recommendation area overview

The Trusted Data Spaces area defines how secure, sovereign and interoperable data sharing[6] underpins MaaS in Europe. It focuses on trusted industrial data spaces, secure EU cloud infrastructure and strong cybersecurity so that industrial data can be shared across companies and borders under clear data-owner control[7].

Priority is given to funding and deploying data spaces based on open, harmonised formats, robust governance and transparent rules aligned with the Data Act and EU digital policy. A sovereign, EU-wide secure cloud should offer encrypted, interoperable and compliance-by-design services.

Cybersecurity is a core design requirement, consistent with the Cyber Resilience Act[8], NIS2 and related standards (e.g. ISO/IEC 27001, IEC 62443). Key elements include risk management, secure communication, identity and key management, tamper-proof logging and certification. Together, trusted data spaces, secure cloud and cybersecurity provide the digital backbone for scalable, resilient MaaS ecosystems and strengthen Europe's industrial autonomy.

Scope

- Creation of a trusted data space for data sharing utilising open data formats that ensures data safety and security responding to the challenges of MaaS business models
- An EC wide secure cloud solution and directed initiatives supporting the uptake of security solutions in SMEs such as blockchain
- Cybersecurity approaches to protect data

---

[6] 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 and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (**Data Act**); creates rules for data access and portability, requiring interoperability standards for connected products and industrial data; The Data Act gives individuals and businesses the right to access the data produced through their utilisation of smart objects, machines and devices;

[7] Regulation (EU) **2022/868** of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (**Data Governance Act**); introduces frameworks for trusted data sharing, including data intermediaries and altruism mechanisms; The Data Governance Act addresses privacy of data, e.g. customer data for personalised products or data being collected through interactions between humans in MaaS production facilities or supply chains

[8] Regulation (EU) **2024/2847** of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (**Cyber Resilience Act**); sets baseline cybersecurity requirements for digital products and services, to be supported by harmonised standards; The Cyber Resilience Act which is important due to the digital nature of products and increased data being recorded, e.g. Product Passports, and interconnectivity between actors in the supply chain

3.1.2. Recommended actions - Trusted Data Spaces ensuring safe and effective cooperation
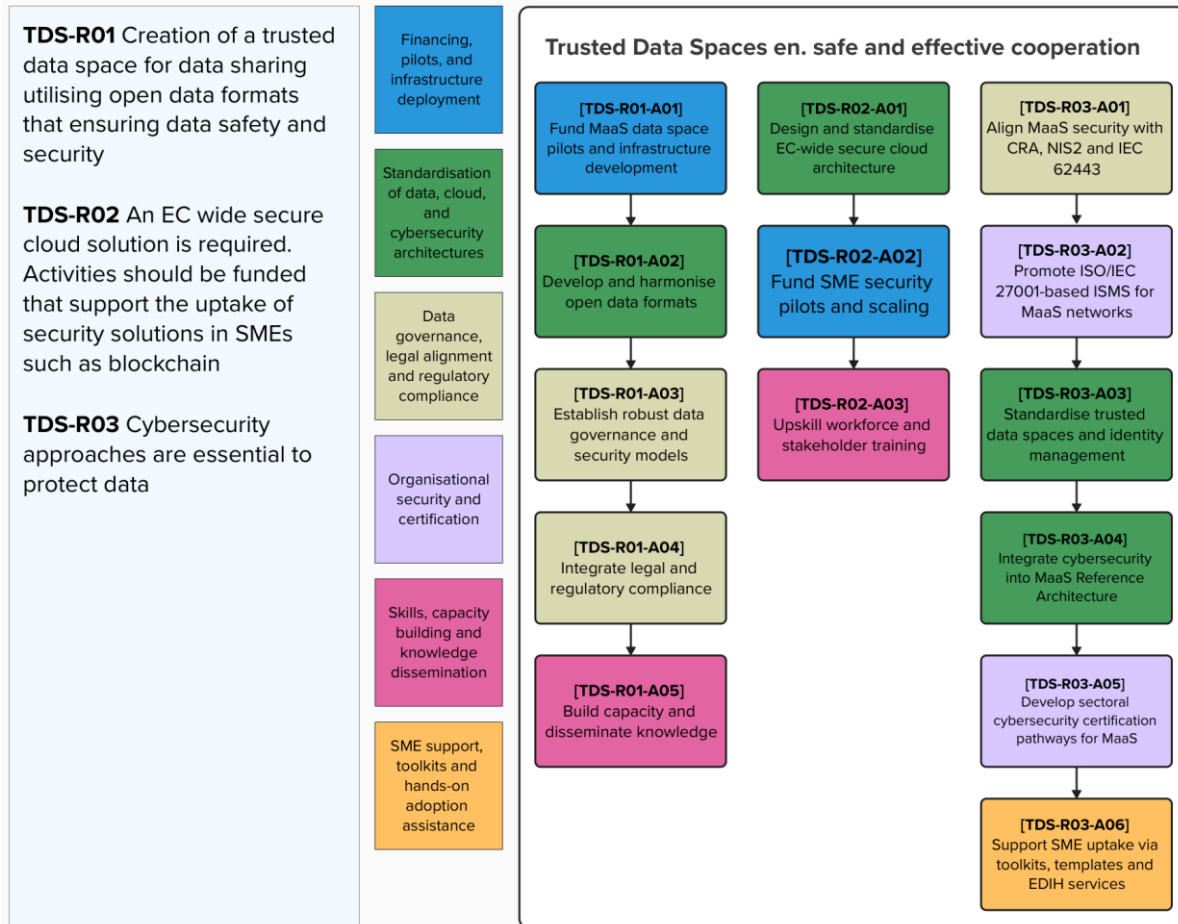
Figure 6. **Trusted Data Spaces** recommended actions

3.1.2.1. Creation of a trusted data space for data sharing utilising open data formats that ensure data safety and security

Funding should support creation of Data Spaces for MaaS based on open, interoperable data formats and secure information exchange.

Trusted data spaces must provide secure access, processing and sharing of industrial information, supported by clear governance, voluntary agreements and EU-compliant legal and contractual frameworks. Governance models should define roles for data producers, consumers and intermediaries and ensure privacy, security and transparency.

Technical infrastructure should include strong security mechanisms (cryptography, authentication, authorisation, audit trails) to protect integrity and prevent unauthorised access.

> **Data Governance Act[9]**
>
> The Data Governance Act is likely to be beneficial, but **for MaaS sector specific dataspaces are required.** It is perceived that there will be a positive impact as uptake of the Data Governance Act will provide rules/guidelines for that can be exploited. It is also good for promoting the concept of data spaces and driving the acceptance of them.

Actions under the recommendation

Name of action	Action description
TDS-R01-A01. Fund MaaS data space pilots and infrastructure development	Launch EU calls (Horizon Europe, Digital Europe) for consortia to design and operate trusted MaaS data spaces with secure, scalable and GDPR/Data Act–compliant architectures, involving large industry, SMEs, technology providers and research.
TDS-R01-A02. Develop and harmonise open data formats	Develop interoperable, modular open data formats for MaaS-relevant information, building on existing standards (IDS-RAM, GAIA-X, CEN/CENELEC, ISO), piloting cross-sector implementations and embedding cybersecurity and identity features.
TDS-R01-A03. Establish robust data governance and security models	Define EU-wide data governance guidelines (roles, consent, contracts, boards) and require strong security measures (encryption, authentication, authorisation, secure APIs and logging) in all data-sharing platforms.
TDS-R01-A04. Integrate legal and regulatory compliance	Ensure data spaces and formats explicitly support compliance with the Data Act, GDPR, NIS2 and sector regulations and promote certified security and interoperability standards.
TDS-R01-A05. Build capacity and disseminate knowledge	Fund training, technical assistance and awareness for SMEs and industrial partners on trusted data spaces. Create online knowledge hubs with best practices, guides and templates via EDIHs and data space support centres.

3.1.2.2. An EC wide secure cloud solution is required. Activities should be funded that support the uptake of security solutions in SMEs such as blockchain

Cybersecurity is crucial for scaling MaaS. Investment is needed in advanced security technologies and staff training.

A unified, EU-wide secure cloud aligned with the Cloud/AI Development Act, Digital Decade, CRA and Data Act should provide interoperable, encrypted and compliance-by-design services. This must serve enterprises of all sizes.

To support SMEs, the EC should fund adoption of security solutions such as blockchain for decentralised, tamper-proof data management, auditability and identity verification. Funding should cover SME onboarding, training and sector-specific solutions that are simple to implement and maintain.

---

[9] Regulation (EU) **2022/868** of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (**Data Governance Act**); introduces frameworks for trusted data sharing, including data intermediaries and altruism mechanisms; The Data Governance Act addresses privacy of data, e.g. customer data for personalised products or data being collected through interactions between humans in MaaS production facilities or supply chains

Name of action	Action description
TDS-R02-A01. Design and standardise EC-wide secure cloud architecture	Define and validate a secure cloud architecture for industrial data spaces with federated identity, open interoperability, end-to-end encryption, blockchain-based auditability and GDPR compliance, developed with CEN/CENELEC JTC 25 and ISO/IEC/ETSI.
TDS-R02-A02. Fund SME security pilots and scaling	Fund SME pilots implementing blockchain-based security, secure cloud onboarding, federated data exchange and DPPs, focusing on usability and compliance-by-design and leveraging EDIHs and existing testbeds.
TDS-R02-A03. Upskill workforce and stakeholder training	Roll out training for SME staff and managers on cyber hygiene, secure cloud use and blockchain traceability, coordinated with EDIHs and EU skills networks and covering technical and organisational risks.

3.1.2.3. Cybersecurity approaches are essential to protect data

Protecting data exchanged within MaaS networks is essential for both information security and trust.

The Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for products with digital elements, and NIS2 extends obligations to many manufacturing enterprises. Standards such as IEC 62443 and ISO/IEC 27001 provide best practices for secure manufacturing systems and supply chains.

Cybersecurity must be embedded in MaaS standardisation: secure communication, identity management, logging, secure development and certification under the European Cybersecurity Certification Framework (ECCF). This protects data integrity and confidentiality, ensures regulatory compliance and builds trust in MaaS platforms.

> **Cyber Resilience Act[10]**
>
> Products with digital elements now need to comply with the Cyber Resilience Act. A key advantage of compliance is that European products can be trusted. This should be promoted more to customers (who may need to pay more for products). The key issue is in providing compliance. **In MaaS supply chains are distributed which means that there is a need to have visibility of what is being incorporated and by whom so that it is possible to certify the product.** Small companies are concerned about complying with the act, and this may stifle innovation. **Guidelines are thus required for industry.**

Actions under the recommendation

Name of action	Action description
TDS-R03-A01. Align MaaS security with CRA, NIS2 and IEC 62443	Create a common MaaS cybersecurity baseline by mapping CRA and NIS2 requirements to IEC 62443 and ISO/IEC 27001 controls, producing sector-specific

---

[10] Regulation (EU) **2024/2847** of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (**Cyber Resilience Act**); sets baseline cybersecurity requirements for digital products and services, to be supported by harmonised standards; The Cyber Resilience Act which is important due to the digital nature of products and increased data being recorded, e.g. Product Passports, and interconnectivity between actors in the supply chain

Name of action	Action description
	Implementation guidelines for secure-by-design, vulnerability handling and supply-chain security.
TDS-R03-A02. Promote ISO/IEC 27001-based ISMS for MaaS networks	Support deployment of ISO/IEC 27001-certified ISMS as the minimum organisational protection for MaaS participants, with an EU guidance profile linking ISO/IEC 27001/27002 to CRA, NIS2 and Data Act/DGA.
TDS-R03-A03. Standardise trusted data spaces and identity management	Specify interoperable security patterns for trusted MaaS data spaces (orders, capabilities, DPPs, sensor data), including identity, access, encryption and usage control. Build reference architectures and APIs for secure connectors, federated identity and tamper-proof logging aligned with CRA and NIS2.
TDS-R03-A04. Integrate cybersecurity into MaaS Reference Architecture	Embed cybersecurity and privacy as cross-cutting layers in MaaS RAM (roles, data flows, building blocks), including secure onboarding, key management, SBOM, monitoring and incident response, reusing AAS and IEC 62443 concepts.
TDS-R03-A05. Develop sectoral cybersecurity certification pathways for MaaS	Use ECCF and EUCC/EUCS to define certification pathways for MaaS components (cloud, IIoT, OT, software), with typical assurance levels and reuse profiles for key MaaS scenarios, complementing CRA conformity assessment.
TDS-R03-A06. Support SME uptake via toolkits, templates and EDIH services	Develop modular cybersecurity toolkits for MaaS SMEs (risk templates, policy sets, SBOM/patch workflows, configuration checklists) aligned with CRA/NIS2/IEC 62443 and deliver them via EDIHs and manufacturing data spaces with hands-on support.

3.1.3. Actions grouped by category

3.1.3.1. Financing, pilots, and infrastructure deployment

Actions focus on financing and piloting secure data spaces and cloud solutions for MaaS.

EU-level funding should support secure MaaS data spaces and SME-driven security innovations, covering GDPR/Data Act–compliant infrastructures, blockchain-based security, secure cloud onboarding, federated data exchange and Digital Product Passports. Activities should emphasise usability, compliance-by-design and use of EDIHs and existing testbeds.

3.1.3.2. Standardisation of data, cloud, and cybersecurity architectures

Actions aim at standardising data formats, cloud architectures and cybersecurity building blocks.

The EC should coordinate development of open data formats, secure cloud architectures and trusted data-space standards. This includes modular data formats, GDPR-compliant cloud architectures with federated identity and encryption, and common security patterns for identity, access, encryption and usage control. Cybersecurity and privacy must be fully integrated into the MaaS Reference Architecture through reference implementations and secure connector models aligned with CRA, NIS2 and EU standards.

3.1.3.3. Data governance, legal alignment and regulatory compliance

Actions define EU-wide governance and cybersecurity frameworks for MaaS data spaces.

Guidelines should cover roles, consent and contractual models, with mandatory security controls (end-to-end encryption, strong authentication, secure APIs, auditing). Data spaces must comply with the Data Act, GDPR, NIS2 and sector rules, using certified security and interoperability standards. CRA and NIS2 obligations should be aligned with IEC 62443 and ISO/IEC 27001 into a practical cybersecurity baseline.

3.1.3.4. Organisational security and certification

Actions address organisational processes, ISMS deployment and certification.

ISO/IEC 27001-based ISMS should be the security baseline for MaaS participants, supported by EU guidance linking ISO/IEC 27001/27002 with CRA, NIS2 and Data Act requirements. Sector-specific cybersecurity certification pathways under ECCF (EUCC/EUCS) should define assurance levels for cloud, IIoT, OT and software, complementing CRA conformity assessment.

3.1.3.5. Skills, capacity building and knowledge dissemination

Actions aim to build skills, awareness and knowledge sharing.

The EC should fund training, technical assistance and knowledge-sharing for SMEs and industrial partners on trusted data spaces, governance, cyber hygiene, secure cloud use and blockchain-based traceability. Online repositories and knowledge hubs, run with EDIHs and data space support centres, should collect best practices, guides and templates.

3.1.3.6. SME support, toolkits and hands-on adoption assistance

Actions provide practical support for SMEs.

The EC should develop modular cybersecurity toolkits aligned with CRA, NIS2 and IEC 62443, covering risk assessment, policies, SBOM, patch management and configuration. EDIHs should offer hands-on support, shared security services and onboarding guidance to enable SMEs to join trusted MaaS ecosystems.

3.2. Interoperability based on data standardisation and digital tools

Resilience in MaaS comes from transparency, prediction and reconfigurability.
When disruptions hit, strength lies in the ability to reshape networks instantly; rerouting production, data and know-how where they're most needed

3.2.1. Recommendation area overview

Given the specific nature of MaaS business models, as well as the requirements for cooperation between stakeholders in value chains, standardisation is an essential element for the further scaling of MaaS in Europe. MaaS further development is possible under the collaborative open federated platform models that are based on open standards and interoperable foundations and solutions. It is crucial to foster a collaborative ecosystem where manufacturers, suppliers, and service providers can work together seamlessly to provide on-demand manufacturing solutions.

Therefore, standards are essential both in the context of driving interoperability within factories to allow exchange of information at machine and manufacturing process level to ensure flexibility and in the context of orders processing and collaboration between different parties in supply chains or more complex marketplaces. Standardisation should therefore address areas such as semantic interoperability for exchange of data as well as common, agreed standards in data management. Building comprehensive partnerships involving multiple partners and requiring seamless data exchange in real time involves ensuring standard solutions at the basic levels of enterprise operations for secure data exchange between companies. Building on this the development of standard reference architectures for MaaS is seen as an important first step. Building such a model would also allow for more targeted and practical solutions to be developed within R&D projects, including those funded by the European Commission.

The Interoperability area defines how MaaS relies on seamless, secure information exchange between machines, factories and organisations. It focuses on machine-level communication standards, company-to-company data exchange and common architectural guidance so heterogeneous systems can work as modular, "plug-and-play" elements in distributed networks.

Priorities include harmonised technical protocols, shared data models and secure digital identities in line with the Machinery Regulation and Data Act. Open, multilingual data formats ensure consistent interpretation of technical and safety information across languages and regions.

Interoperability also covers tools and architectures. Open trade-off analysis tools should connect cost, lifecycle and sustainability data for joint optimisation. A MaaS Reference Architecture Model should align frameworks such as RAMI 4.0, IDS-RAM, GAIA-X and IIRA, providing a coherent blueprint for roles, data flows and components.

AI Act[11]

The AI Act has significant impact as AI is being used everywhere (customer interface, manufacturing process, supply chain and in circularity). However, there is a lack of best practice and guidelines for implementation concerning the different levels of AI being used in the MaaS value chain, e.g. personal data for the customer interface and potential safety issues in manufacturing machinery/cobots. Guidelines and best practice for MaaS are thus needed. It would also be useful to create a map of MaaS and uses of AI. At the same time there is a need to investigate how to minimise the data being used. AI requires lots of data, but this needs to be reduced as much as possible.

The AI Act is perceived to be **more important for SMEs as they are concerned about breaking the law. This is a potential inhibitor to innovation. Tools are required to easily check that usage of AI is in alignment with the act.** Larger companies have the resources to check compliance and experiment with AI.

Scope

- Standardisation and open tools enabling seamless exchange of information between companies to allow collaboration and enable interoperability within MaaS ecosystems, including common semantics and multilingual data formats
- Standardisation for interoperability to allow exchange of information at machine and processes level including ordering, matchmaking, service description / service catalogues, process/manufacturing capabilities
- Reference Architecture Model for MaaS

---

[11] 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**); defines risk-based requirements for AI systems, again depending on standards for implementation; The AI Act which classifies AI into risk categories Prohibited AI, High Risk AI, Limited Risk AI and Minimal Risk AI. Potentially due to the nature of manufacturing machinery and cobots interacting with humans it is likely that applications will fall under the High-Risk AI category. The Act also provides requirements for transparency and disclosure for generative AI

3.2.2. Recommended actions - Interoperability based on data standardisation and digital tools
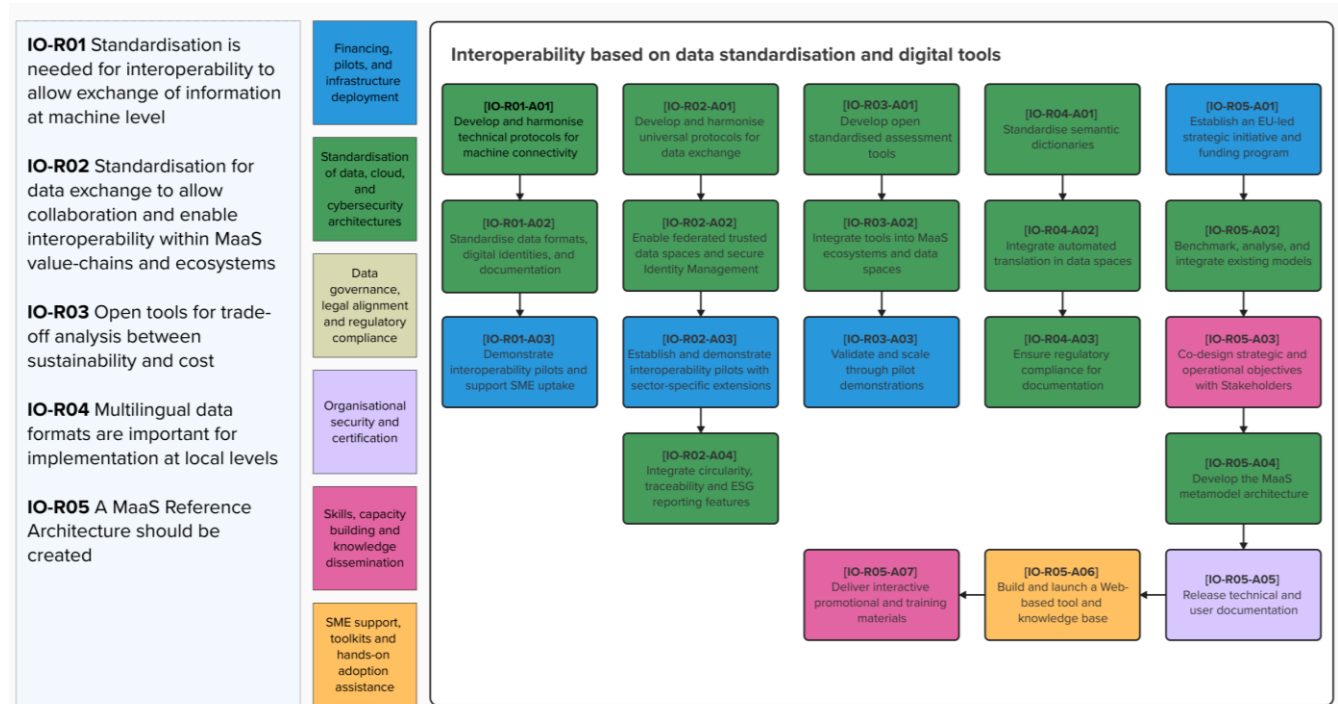
Figure 7. **Interoperability** recommended actions

3.2.2.1. Standardisation is needed for interoperability to allow exchange of information at machine level

Standardisation should enable seamless machine-level information exchange, guided by EU Machinery Regulation 2023/1230 and its focus on AI, cybersecurity and digital twins.

This includes harmonised connectivity protocols, unified data formats, secure digital identities and documentation. In MaaS, these standards support modular, "plug-and-play" integration, real-time visibility, remote management and flexible reconfiguration, while digital documentation and audit trails reduce administrative burden.

Actions under the recommendation

Name of action	Action description
IO-R01-A01. Develop and harmonise technical protocols for machine connectivity	Establish harmonised communication protocols (e.g. OPC UA, AAS, RAMI 4.0 layers) for interoperable M2M connectivity, referencing Machinery Regulation 2023/1230 and prioritising vendor-neutral APIs and semantic interoperability.
IO-R01-A02. Standardise data formats, digital identities, and documentation	Standardise machine data formats, secure digital identities (e.g. EN IEC 61406) and digital documentation frameworks, including support for multilingual exchange and traceability and remote audits.
IO-R01-A03. Demonstrate interoperability pilots and support SME uptake	Deploy pilots showing machine-level interoperability in real MaaS networks, especially multi-vendor SME environments, and provide open toolkits and implementations via labs and living labs.

3.2.2.2. Standardisation for data exchange to allow collaboration and enable interoperability within MaaS value-chains and ecosystems

MaaS ecosystems need standards that support secure, real-time data exchange between machines, modules and platforms, independent of manufacturer or location.

Common protocols and harmonised data formats (e.g. OPC UA Companion Specifications, Weihenstephan Standards) must ensure reliable machine-to-machine and enterprise data flows. Coordination with EU initiatives (e.g. Data Act) and sector frameworks will enable flexible integration, traceability and automation, increasing efficiency and scalability.

Actions under the recommendation

Name of action	Action description
IO-R02-A01. Develop and harmonise universal protocols for data exchange	Create a harmonised set of protocols for cross-company data sharing using OPC UA Companion Specifications, Weihenstephan Standards and open APIs, including standardised semantic models, metadata and machine-readable contracts aligned with the Data Act/DGA.
IO-R02-A02. Enable federated trusted data spaces and secure identity management	Promote federated, trusted data spaces (IDS, GAIA-X, Catena-X) where partners keep control and compliance while exchanging sensitive data, using standardised secure identities, access control and credentialing (eIDAS2, ISO/IEC 15459).
IO-R02-A03. Establish and demonstrate interoperability pilots with sector-specific extensions	Run pilots to refine interoperability standards with sector-specific extensions, focusing on real multi-partner use cases and aligning with European and international SDOs.
IO-R02-A04. Integrate circularity, traceability and ESG reporting features	Embed lifecycle tracking, circularity, DPP support and automated ESG reporting into interoperability frameworks to enable sustainable manufacturing and regulatory compliance.

3.2.2.3. Open tools for trade-off analysis between sustainability and cost

Open tools combining real-time data, Life Cycle Assessment and cost modelling are crucial for companies to assess both environmental and economic impacts of production choices. This aspect is highly important for MaaS business models aspiring to follow Twin Transition principles.

Integrated into MaaS ecosystems, these tools should help stakeholders compare materials, processes and suppliers using **clear metrics** and visual dashboards, enabling transparent and collaborative decision-making that supports greener, competitive manufacturing.

Actions under the recommendation

Name of action	Action description
IO-R03-A01. Develop open standardised assessment tools	Develop open-source, API-based tools that combine real-time manufacturing data with standardised LCA and LCC models to calculate CO_2 footprints and cost impacts, referencing ISO 14040/14044.
IO-R03-A02. Integrate tools into MaaS ecosystems and data spaces	Integrate trade-off tools into MaaS platforms and European data spaces, connecting to material banks and supplier sustainability data and supporting DPP deployment.

Name of action	Action description
IO-R03-A03. Validate and scale through pilot demonstrations	Launch SME-focused pilots to demonstrate the commercial value and usability of sustainability-cost trade-off tools in real MaaS scenarios and support regulatory compliance.

3.2.2.4. Multilingual data formats are important for implementation at local levels

To scale MaaS in Europe, multilingual data formats are needed for safety information, manuals and technical documentation, in line with Machinery Regulation (EU) 2023/1230.

Standardised, multilingual and quality-controlled data formats and terminology support compliance, reduce risk and enable cross-border cooperation. Embedding these capabilities in digital infrastructures and documentation speeds partner onboarding and service deployment across all regions.

Actions under the recommendation

Name of action	Action description
IO-R04-A01. Standardise semantic dictionaries	Adopt semantic standards such as IEC 61360 and ISO 13584 to define manufacturing properties in machine-readable, multilingual form, enabling automatic interpretation across languages.
IO-R04-A02. Integrate automated translation in data spaces	Embed automated, quality-assured translation services into EU data spaces to support real-time localisation of MaaS interfaces and documentation and reduce linguistic barriers for SMEs.
IO-R04-A03. Ensure regulatory compliance for documentation	Develop digital workflows that automatically generate user manuals and safety instructions in local languages in line with Machinery Regulation 2023/1230, reducing liability and improving safety.

3.2.2.5. A MaaS Reference Architecture should be created

A Reference Architecture Model for MaaS (MaaS RAM) should bridge interoperability and data-exchange gaps by providing a harmonised blueprint for business models, system architecture and enterprise integration in cooperative networks.

MaaS RAM should consolidate technical specifications and standards (data formats, semantics, cybersecurity), align SMEs and large enterprises, and streamline compliance with EU requirements. It must be actionable and scalable, offering high-level guidance and practical tools.

Relation to RAMI 4.0, IDS-RAM, and other metamodels

1. RAMI 4.0: MaaS RAM should reuse RAMI's modularity, interoperability and automation principles, adapted to service-centric, distributed manufacturing,
2. IDS-RAM: MaaS RAM should build on IDS-RAM for secure, sovereign and interoperable data exchange,
3. IIRA, FIWARE, GAIA-X: MaaS RAM should draw from their best practices on platform interoperability, modularity and distributed services to ensure cross-domain compatibility.

Standardisation bodies and pilot actions (MASTT2040 and sister projects) should jointly align technical, legal and operational aspects.

A MaaS Reference Architecture would be highly beneficial, and this could be done in stages, firstly through national standards bodies, e.g. DIN and MaaS projects, and then at EC level. Here there is support for creation of Technical Committee as currently there is no technical committee that covers

MaaS. It will be necessary to bring together industry, ethics/rights and government actors. A MaaS reference architecture could be started through DIN via a CWA with consultation of MaaS projects.

Other positive actions would be to subcontract SDOs into future projects or have them as partners. The aim of this would be to translate results into new standards items. One approach would be to specifically include SDO participation in the call.

Actions under the recommendation

Name of action	Action description
IO-R05-A01. Establish an EU-led strategic initiative and funding program	Launch a flagship Horizon Europe programme to develop MaaS RAM with clear milestones, covering research, standardisation, tools, stakeholder consultation and training/promotional outputs.
IO-R05-A02. Benchmark, analyse, and integrate existing models	Assemble experts from SDOs, agencies, industry and academia to analyse and integrate MaaS concepts with RAMI 4.0, IDS-RAM and other models, identifying convergence points and gaps and avoiding duplication.
IO-R05-A03. Co-design strategic and operational objectives with Stakeholders	Organise workshops and consultations with SMEs, large industry, vendors and DIHs to define how MaaS RAM should serve different stakeholders and business models, ensuring input from existing architecture teams.
IO-R05-A04. Develop the MaaS metamodel architecture	Draft and publish a meta-architecture covering functional, information and process views, specifying layers for interoperability, sovereignty, security, modularity and service orchestration.
IO-R05-A05. Release technical and user documentation	Prepare technical specifications and implementation guides, with modular documentation sets (developer kits, integrator guides, compliance checklists) for SMEs and large enterprises.
IO-R05-A06. Build and launch a Web-based tool and knowledge base	Develop a public web application with an interactive MaaS RAM knowledge base, use cases, standards mapping and self-assessment and planning tools.
IO-R05-A07. Deliver interactive promotional and training materials	Produce digital campaigns and modular training materials for industry, regulators, academia and SMEs and deliver webinars, demos and workshops via EDIHs and partner networks.

3.2.3. Actions grouped by category

3.2.3.1. Financing, pilots, and infrastructure deployment

Actions focus on pilots and infrastructure for interoperable MaaS solutions.

The EC should fund coordinated pilots that demonstrate multi-vendor interoperability, validate sector extensions and test sustainability-cost tools, with strong SME involvement. A flagship Horizon Europe initiative should support large-scale demonstrations, reference implementations, coordination and knowledge transfer via labs and living labs.

3.2.3.2. Standardisation of data, cloud, and cybersecurity architectures

Actions standardise protocols, data formats, semantic models and identities.

The EC should establish a harmonised technical basis for MaaS: machine connectivity protocols, semantic models and secure identities aligned with OPC UA, AAS, IEC/ISO dictionaries and multilingual standards. Trusted federated data spaces should ensure data sovereignty. Circularity, traceability, ESG

reporting and automated compliance must be integrated. Benchmarking against RAMI 4.0 and IDS-RAM should lead to a coherent MaaS metamodel architecture.

3.2.3.3. Organisational security and certification

Actions focus on documentation, implementation guides and toolkits for MaaS RAM.

The EC should provide clear technical specifications and user-oriented documentation for MaaS RAM, including modular guides, toolkits and compliance checklists for SMEs and large enterprises, ensuring consistent adoption and conformity with EU rules.

3.2.3.4. Skills, capacity building and knowledge dissemination

Actions support stakeholder engagement and knowledge transfer.

The EC should organise structured consultations, expert workshops and co-design sessions with industry, SMEs, technology providers and standardisation bodies to align requirements and build common understanding of MaaS RAM.

3.2.3.5. SME support, toolkits and hands-on adoption assistance

Actions provide practical tools and a central platform.

A public web platform should host MaaS RAM, standards, integration guides and self-assessment tools. Promotional and training materials, distributed via EDIHs and partner networks, should target SMEs, industry, regulators and academia to speed implementation.

3.2. Circular Economy enabled MaaS

To be truly transformative it is crucial for future MaaS business models to be tightly integrated with Circular Economy principles

What used to be waste becomes discoverable input, enabling components recovery, requalification, and redeployment within the same MaaS network, though circularity won't happen by design alone. It requires transparent value chains, digital passports, and shared accountability across every R-cycle interaction

3.3.1. Recommendation area overview

Manufacturing-as-a-Service business models offer advantages with respect to resilience of supply chain. However, the benefits of implementing MaaS business models can only be achieved through the gradual implementation of ecosystem solutions that ensure efficient coordination and transparency within the value chains being created. Data management and standardisation appear to be important elements in ensuring such transparency, from product design through sourcing raw materials and manufacturing processes to life cycle monitoring. Importantly, in the circular economy of the future, the number of such cycles for a given product will increase due to new models based not only on recycling, but also on renewal and reuse. This raises questions and highlights the challenges associated with the responsibility for maintaining data, ensuring its security and compliance, often for decades. Given the complexity of the circular economy issue, also in the context of stakeholders, actions aimed at ensuring its future achievement should be gradual but decisive, and supported by regulations implemented sensibly and taking into account the needs of various groups, including SMEs in particular.

The Circular Economy area aims to embed sustainability, durability and circularity into MaaS through coherent standards, eco-design rules and Digital Product Passports (DPPs[12]). Key priorities are eco-design standards under ESPR that reduce hazardous substances, enable repair and recycling, and consider SME capabilities. Harmonised standards should support certification and eco labels to make circular performance visible. DPPs are central for lifecycle traceability and trustworthy sustainability data. Interoperable, standardised data formats, supported by funding for pilots and training, are needed. Together, eco-design, product policy and digital transparency create measurable, scalable circular practices aligned with EU climate and competitiveness goals.

Scope

- Eco design standards for MaaS
- Standards, and eco labels for sustainable/circular products along with certification in MaaS value chains
- Digital Product Passports

---

[12] **Digital Product Passport (DPP)** – a core tool of the Circular Economy Action Plan, requiring product data standards to enable reuse, repair and recycling; Product Passports will be a key driver for circularity requiring collection of data throughout a products life. The general requirements for digital product passports include having a data carrier on the product, its packaging or on documentation, with a unique product identifier according to ISO/IEC 15459:2015. This needs to be in an interoperable machine-readable, structured, and searchable format with information on the product model, batch, or item

3.3.2. Recommended actions - Circular Economy enabled MaaS

CE-R01 Eco design standards for Manufacturing-as-a-Service

CE-R02 European standards, and eco labels for sustainable/circular products along with certification

CE-R03 Digital Product Passports are required for transparency. The data format should be reviewed by industry associations and standardised
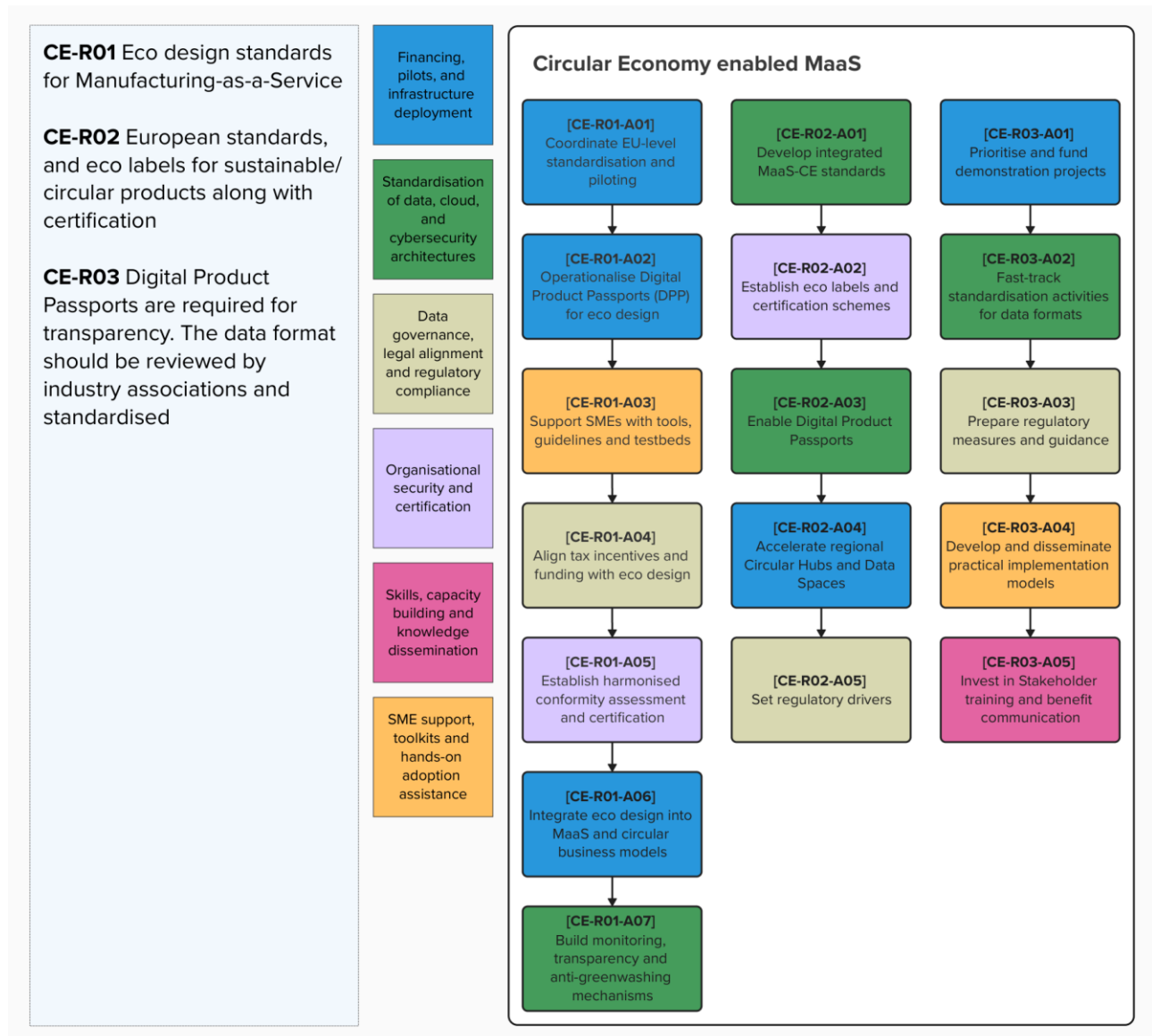
Figure 8. **Circular Economy enabled MaaS** recommended actions

3.3.2.1. Eco design standards for Manufacturing-as-a-Service

Eco-design standards should be developed and supported by pilot projects, tools and national tax incentives that promote circular production.

These standards must address hazardous substance reduction, recycled materials, ease of disassembly and repair, refurbishment and recycling, in line with ESPR. Stakeholder consultation and impact assessment should balance industry feasibility with ambitious sustainability targets, prioritising high-impact sectors.

SMEs need tailored guidelines and support to comply, with possible simplifications for micro and small enterprises. Horizontal rules for material groups can create synergies. Overall, eco-design standards will drive markets for repairable, recyclable products and support EU energy, circular economy and decarbonisation objectives.

> **Digital Product Passports[13]**
>
> Digital Product Passports are seen as essential to support circularity. These need to be introduced in a **sector specific manner.** A key challenge is maintaining the Product Passport data for 20-30 years as companies may disappear in this time frame. A mechanism needs to be set up to independently store data.

Actions under the recommendation

Name of action	Action description
CE-R01-A01. Coordinate EU-level standardisation and piloting	Mandate CEN-CENELEC-ETSI to develop eco-design standards (durability, reparability, recyclability, recycled content, CRM reduction, hazardous substances) for MaaS-relevant products and fund pilots that test methods and tools in real MaaS settings, feeding results into standardisation.
CE-R01-A02. Operationalise Digital Product Passports (DPP) for eco design	Develop standardised DPP data models/interfaces under ESPR Article 10, encoding eco-design parameters (repairability, recycled content, CRM use). Fund pilots that integrate DPP generation into CAD/PLM/ERP/MES workflows on MaaS platforms.
CE-R01-A03. Support SMEs with tools, guidelines and testbeds	Provide open, modular eco-design toolkits (LCA templates, disassembly checklists, material assistants) for SMEs, integrated with digital engineering tools, and operate regional eco-design testbeds via EDIHs.
CE-R01-A04. Align tax incentives and funding with eco design	Encourage Member States to introduce tax incentives for eco-designed products and circular equipment and use compliance or piloting of standards as a positive criterion in EU/national funding calls.
CE-R01-A05. Establish harmonised conformity assessment and certification	Develop harmonised conformity assessment for eco-design requirements with simplified options for SMEs, build lab competence for circularity testing and link schemes to eco labels.
CE-R01-A06. Integrate eco design into MaaS and circular business models	Create guidelines for embedding eco-design standards in MaaS contracts, platform rules and lifecycle services (e.g. Product-Lifecycle-as-a-Service) and fund demonstrators that measure cost, lead-time, material and CO_2 impacts.
CE-R01-A07. Build monitoring, transparency and anti-greenwashing mechanisms	Develop EU methodologies and indicators for eco-design performance aligned with environmental KPIs and PEF and embed them in standards and DPPs. Implement phased mandatory reporting of core circularity indicators via a single EU portal.

3.3.2.2. European standards, and eco labels for sustainable/circular products along with certification

Europe should develop harmonised MaaS-CE standards focusing on environmental performance, lifecycle traceability and circularity. These should underpin certification and eco labels that are clear,

---

[13] **Digital Product Passport (DPP)** – a core tool of the Circular Economy Action Plan, requiring product data standards to enable reuse, repair and recycling; Product Passports will be a key driver for circularity requiring collection of data throughout a products life. The general requirements for digital product passports include having a data carrier on the product, its packaging or on documentation, with a unique product identifier according to ISO/IEC 15459:2015. This needs to be in an interoperable machine-readable, structured, and searchable format with information on the product model, batch, or item

trusted and linked to DPPs, ensuring sustainability claims are verifiable and traceable. This will build consumer confidence, open new markets and strengthen strategic autonomy.

Actions under the recommendation

Name of action	Action description
CE-R02-A01. Develop integrated MaaS-CE standards	Launch joint working groups to harmonise circular economy, eco-design and sustainable manufacturing standards for MaaS, covering modular product design, lifecycle tracking, material banks and interoperability.
CE-R02-A02. Establish eco labels and certification schemes	Define eco labels for circular MaaS products with clear verification and create a unified certification framework linked to standards and DPPs, with accessible third-party verification for SMEs.
CE-R02-A03. Enable Digital Product Passports	Co-design interoperable DPP data models capturing circularity, traceability and sustainability indicators, and mandate DPP adoption in priority sectors (e.g. electronics, batteries).
CE-R02-A04. Accelerate regional Circular Hubs and Data Spaces	Fund digital circular trade hubs for local repair, reuse and remanufacturing and secure data spaces for critical material recovery and lifecycle collaboration.
CE-R02-A05. Set regulatory drivers	Introduce mandatory ESG reporting linked to eco labels and DPPs and align incentives and green public procurement with certified circular MaaS products.

3.3.2.3. Digital Product Passports are required for transparency. The data format should be reviewed by industry associations and standardised

It is important to undertake further actions at a EU level, including funding directed projects focused on the development of interoperable methods for data collection and secure exchange of reliable information in DPPs. Given that many activities in the area of DPP are already underway, it is important that projects take into account the requirements of MaaS business models at an early stage and that they include the aspects of industry-led standardisation and ensure strong SME focus. Regulatory measures should accelerate DPP adoption, with clear requirements that support circular practices. Training materials and sector-specific use cases must build implementation capacity.

Priority initiatives in key sectors should produce detailed implementation models that turn regulatory and technical requirements into practical SME guidance, showing business incentives, integration templates and lessons learned. Actions should begin quickly to maximise circularity and competitiveness.

Actions under the recommendation

Name of action	Action description
CE-R03-A01. Prioritise and fund demonstration projects	Launch calls for projects piloting advanced DPP data collection and exchange in real supply chains, especially SME-focused and involving SDOs, industry consortia and data-space facilitators to create scalable reference solutions.
CE-R03-A02. Fast-track standardisation activities for data formats	Work with industry and SDOs to accelerate interoperable DPP data models (CEN JTC 24, ISO/IEC 15459, IEC, Catena-X, GS1), synchronising sector pilots and identifying common cross-sector requirements.
CE-R03-A03. Prepare regulatory measures and guidance	Prepare regulation making DPP mandatory for priority product groups with phased timelines and clear criteria for reliable data, transparency, data protection, IP and confidentiality.

Name of action	Action description
CE-R03-A04. Develop and disseminate practical implementation models	Fund projects to produce detailed SME-focused DPP use cases, handbooks, cost/benefit analyses and technical templates and disseminate them via SME networks and EDIHs.
CE-R03-A05. Invest in Stakeholder training and benefit communication	Create training for SME staff, integrators and supply chain managers on implementing standardised DPPs, focusing on data quality, security and business value, and communicate benefits using results from pilots.

3.3.3. Actions grouped by category

3.3.3.1. Financing, pilots, and infrastructure deployment

Actions fund large-scale pilots, test infrastructures and regional deployment.

Investment should support eco-design standards, interoperable DPP models and circular-ready product architectures in real industrial settings. Demonstrations should connect eco-design tools with engineering and MaaS platforms and strengthen regional circular hubs and data spaces. Scalable DPP pilots should act as reference implementations.

3.3.3.2. Standardisation of data, cloud, and cybersecurity architectures

Actions develop harmonised data and semantic standards for circular MaaS.

Lifecycle and environmental indicators should be embedded into DPP models and interoperable data formats to ensure transparent, traceable information. MaaS-CE standards must support lifecycle tracking, material reuse and distributed manufacturing. Coordinated DPP schemas across sectors should avoid fragmentation and build a coherent technical base.

3.3.3.3. Data governance, legal alignment and regulatory compliance

Actions establish coherent governance and regulatory alignment for circular data flows.

Incentive frameworks and market rules should encourage eco-design and circularity. Regulatory drivers should ensure consistent ESG and lifecycle reporting and define mandatory DPP use with clear data and confidentiality requirements, giving predictable compliance paths.

3.3.3.4. Organisational security and certification

Actions develop harmonised certification and conformity assessment for circularity.

Unified eco labels and verification protocols should evaluate durability, repairability and material efficiency. Conformity procedures and third-party testing must be accessible to SMEs, providing reliable evidence of performance and alignment with standards and DPP rules.

3.3.3.5. Skills, capacity building and knowledge dissemination

Actions support training and communication for DPP implementation.

Capacity-building programmes should improve understanding of data quality, security and the value of standardised DPPs for technical and management audiences. Communication should highlight business benefits, using pilot results to demonstrate feasibility.

3.3.3.6. SME support, toolkits and hands-on adoption assistance

Actions provide practical tools and models for SMEs.

Modular toolkits (LCA templates, design-for-disassembly guides, material selection aids) should integrate with common engineering tools. Practical models and use cases should explain costs, benefits and DPP deployment steps. Shared testbeds and good-practice resources can support experimentation and rapid adoption.

3.4. Regulation

3.4.1. Recommendation area overview

The Regulation area describes how EU rules for reporting, certification and safety should support trustworthy MaaS.

First, mandatory disclosure and transparency via ESG reporting and DPPs enable traceable and comparable environmental, social and governance data, supporting investment, procurement and market access decisions.

Second, robust certification regimes for MaaS value chains and components, including safety, zero waste and quality assurance passports, verify compliance with harmonised benchmarks for security, circularity, emissions, social issues and resilience.

Third, updated occupational health and safety (OHS) rules for highly automated, cobot-rich workplaces embed risk management and worker protection into MaaS operations. Together, these measures align MaaS with the Green Deal, circular economy and digital law.

Environmental, Social and Governance reporting

The introduction of mandatory Environmental, Social and Governance reporting going beyond existing Corporate Sustainability Reporting is seen as a positive move. There needs to be research into how best to do this, firstly to identify the data required to really evaluate this and secondly to minimise the overhead in reporting, so that it is easy for companies to collect data. Without this, future regulation in this area could be seen as an inhibitor rather than beneficial to industry.

Scope

- Mandatory ESG (environmental, social and governance) reporting is required. The EC should introduce regulation to make reporting of a key subset of sustainability data mandatory with a phased 3-year introduction. This should be introduced for different product groups and then expanded over time
- Certification is required for MaaS value chains (e.g. ISO27001), also considering emissions, social, and economic factors, and certification of MaaS components
- Certification is required to prevent unsafe products being produced by MaaS value chains
- Zero waste certification is required to move industry towards circular approaches
- Europe should introduce regulation encouraging the uptake of Digital Product Passports to strengthen recovery of critical raw materials and circular approaches
- With increased automation and cobots there is a need to also consider regulation for occupational health and safety
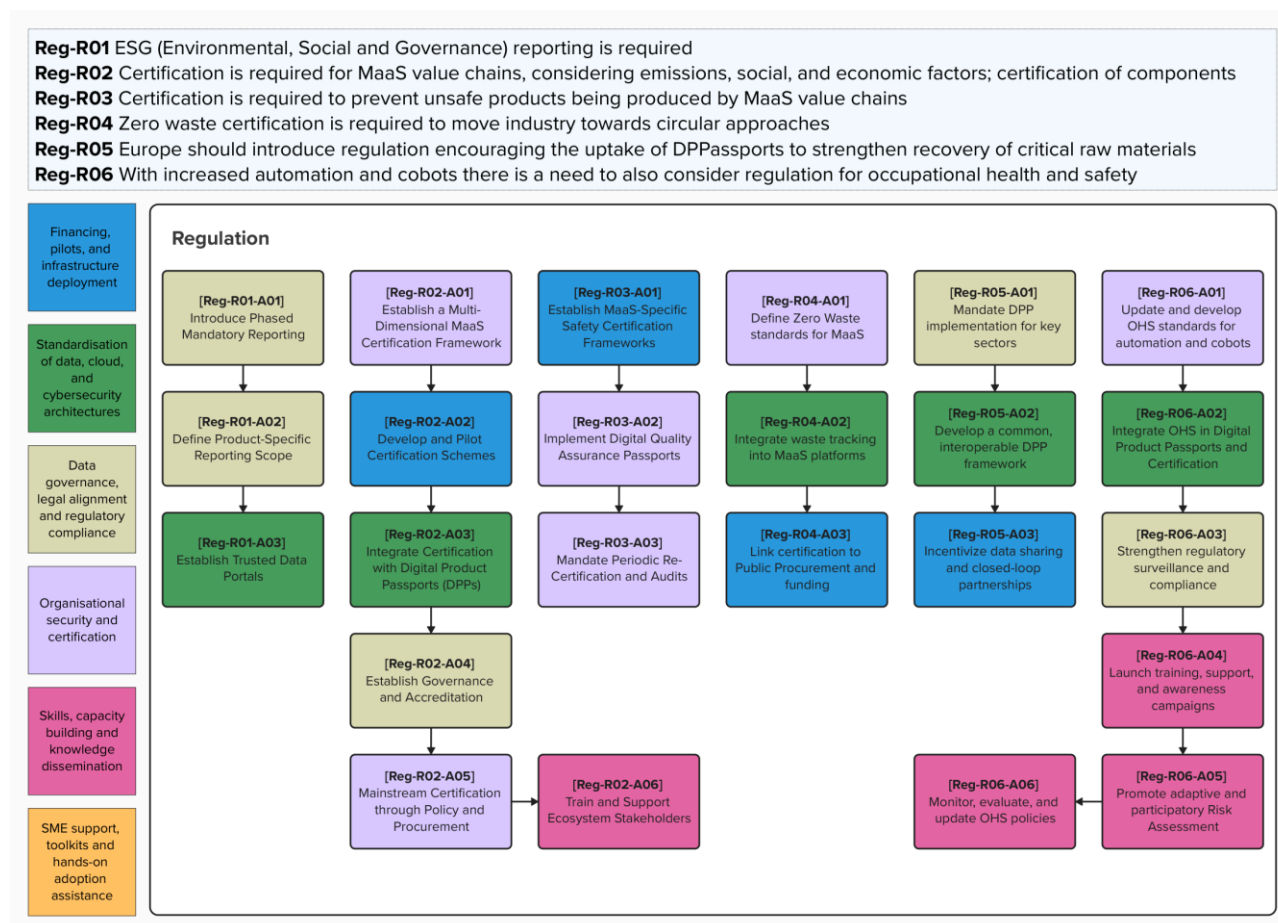
3.4.2. Recommended actions - Regulation

Reg-R01 ESG (Environmental, Social and Governance) reporting is required
Reg-R02 Certification is required for MaaS value chains, considering emissions, social, and economic factors; certification of components
Reg-R03 Certification is required to prevent unsafe products being produced by MaaS value chains
Reg-R04 Zero waste certification is required to move industry towards circular approaches
Reg-R05 Europe should introduce regulation encouraging the uptake of DPPassports to strengthen recovery of critical raw materials
Reg-R06 With increased automation and cobots there is a need to also consider regulation for occupational health and safety

Figure 9. **Regulation** recommended actions

3.4.2.1. Mandatory ESG (environmental, social and governance) reporting is required. The EC should introduce regulation to make reporting of a key subset of sustainability data mandatory with a phased 3-year introduction

Mandatory ESG reporting is needed to support the Green Deal and Circular Economy.

Standardised, mandatory disclosure of sustainability data (e.g. CO_2, resource use, social impact) will combat greenwashing and ensure comparability across supply chains. This aligns with CSRD and ESPR, making sustainability a core business metric. A phased 3-year introduction gives companies, especially SMEs, time to adapt.

Actions under the recommendation

Name of action	Action description
Reg-R01-A01. Introduce Phased Mandatory Reporting	Introduce regulation making a key subset of sustainability data mandatory, with a phased 3-year period allowing companies to start with average figures and gradually move to primary data, easing SME compliance.

Name of action	Action description
Reg-R01-A02. Define Product-Specific Reporting Scope	Begin reporting with high-impact product groups (e.g. batteries, textiles, electronics) and expand over time, using lessons learned to refine requirements.
Reg-R01-A03. Establish Trusted Data Portals	Create a single central EU portal for sustainability data submission so companies report once and share securely with authorities, customers and suppliers.

3.4.2.2. Certification is required for MaaS value chains (e.g. ISO27001), also considering emissions, social, and economic factors, and certification of MaaS components

The complexity of MaaS value chains requires comprehensive certification that covers information security and environmental, social and economic dimensions.

Certification should ensure that processes, products and components meet recognised benchmarks for sustainability, safety, labour practices and economic resilience. Linking certification to DPPs and ESG reporting strengthens transparency and competitive advantage and supports continuous improvement under EU climate, digital and social goals.

Actions under the recommendation

Name of action	Action description
Reg-R02-A01. Establish a Multi-Dimensional MaaS Certification Framework	Develop a comprehensive MaaS certification framework integrating security, environmental, social and economic metrics, aligned with international standards and interoperable with DPPs and ESG reporting.
Reg-R02-A02. Develop and Pilot Certification Schemes	Run EU-wide pilot certification projects with SMEs, large firms and platform providers, creating sector-specific schemes and best-practice guidelines for implementation and renewal.
Reg-R02-A03. Integrate Certification with Digital Product Passports (DPPs)	Embed MaaS certification results into DPPs and develop digital tools for automated compliance and certification tracking across lifecycles.
Reg-R02-A04. Establish Governance and Accreditation	Empower accredited bodies to audit MaaS value chains and promote mutual recognition of certificates across the Single Market and key partners.
Reg-R02-A05. Mainstream Certification through Policy and Procurement	Make EU funding, public procurement and strategic partnerships conditional on MaaS certification, updating criteria with new standards and regulatory demands.
Reg-R02-A06. Train and Support Ecosystem Stakeholders	Develop competence frameworks and training for auditors, managers and SME staff and provide targeted support and incentives for smaller enterprises.

3.4.2.3. Certification is required to prevent unsafe products being produced by MaaS value chains

Flexible MaaS networks can introduce safety risks if controls are weak.

Mandatory safety certification schemes for MaaS value chains should ensure every step, from design to delivery, meets strict safety and quality standards. This is especially important for high-risk sectors (aerospace, automotive, medical). Certification should cover both final products and underlying processes and digital infrastructures.

Name of action	Action description
Reg-R03-A01. Establish MaaS-Specific Safety Certification Frameworks	Create and mandate safety certification frameworks tailored to distributed MaaS networks, covering both individual suppliers and full value chains.
Reg-R03-A02. Implement Digital Quality Assurance Passports	Introduce digital QA passports capturing compliance data across the production lifecycle, providing proof of certification and enabling automated checks.
Reg-R03-A03. Mandate Periodic Re-Certification and Audits	Require regular re-certification and random audits to ensure ongoing compliance in dynamic MaaS networks.

3.4.2.4. Zero waste certification is required to move industry towards circular approaches

To foster circularity, MaaS networks should be guided by "zero waste" objectives.

A Zero Waste Certification scheme should require strong waste minimisation, reuse, remanufacturing and high-value recycling. Real-time waste tracking integrated into MaaS platforms will support "waste-to-resource" value chains. Making certification a requirement for public tenders and key contracts provides strong market incentives.

Actions under the recommendation

Name of action	Action description
Reg-R04-A01. Define Zero Waste standards for MaaS	Define a quantifiable Zero Waste standard for distributed manufacturing, including waste thresholds, reuse rates and end-of-waste criteria.
Reg-R04-A02. Integrate waste tracking into MaaS platforms	Mandate waste tracking modules linked to DPPs in MaaS platforms to monitor material flows and waste in real time and support industrial symbiosis.
Reg-R04-A03. Link certification to Public Procurement and funding	Make Zero Waste Certification a condition for EU funding and public procurement, accelerating adoption of circular practices.

3.4.2.5. Europe should introduce regulation encouraging the uptake of Digital Product Passports to strengthen recovery of critical raw materials and circular approaches

DPPs are crucial for tracking critical raw materials and supporting circularity.

Mandatory DPP adoption would ensure each product carries a digital record of material content, origin, repair history and recycling potential, enabling efficient recovery and reuse. This supports ESPR and the Circular Economy Action Plan, strengthens resource security and supports circular business models.

Actions under the recommendation

Name of action	Action description
Reg-R05-A01. Mandate DPP implementation for key sectors	Introduce regulation requiring DPPs for high-impact product groups, specifying minimum data on critical raw materials, circularity and traceability.
Reg-R05-A02. Develop a common, interoperable DPP framework	Establish technical standards for structured data, semantics and secure exchange protocols so DPPs work across MaaS platforms and data spaces.
Reg-R05-A03. Incentivise data sharing and closed-loop partnerships	Provide financial and regulatory incentives for high-quality DPP data and participation in closed-loop recovery networks, including Horizon Europe funding and procurement preferences.

3.4.2.6. With increased automation and cobots there is a need to also consider regulation for occupational health and safety

Automation and cobots create new physical, cyber-physical and psychosocial risks.

Existing OHS regulations are insufficient for dynamic MaaS workplaces. New, flexible, risk-based regulations and standards must address safety-by-design, psychosocial health, fair work organisation and continuous skill adaptation. OHS requirements should be integrated throughout the MaaS value chain and supported by modern monitoring tools, digital twins and predictive analytics.

Actions under the recommendation

Name of action	Action description
Reg-R06-A01. Update and develop OHS standards for automation and cobots	Revise and develop standards addressing risks from automation and cobots (safety, ergonomics, robotics, AI), including cognitive and psychosocial risks.
Reg-R06-A02. Integrate OHS in Digital Product Passports and Certification	Make OHS controls and compliance visible in DPPs for machines and MaaS platforms and embed OHS requirements into MaaS certification.
Reg-R06-A03. Strengthen regulatory surveillance and compliance	Modernise oversight with digital audit tools and real-time reporting and define clear procedures for incidents and continuous OHS improvement.
Reg-R06-A04. Launch training, support, and awareness campaigns	Provide training and guidelines on safe human-robot collaboration, focusing on SMEs and less digitally mature regions and supporting lifelong upskilling.
Reg-R06-A05. Promote adaptive and participatory Risk Assessment	Encourage participatory risk assessment methods addressing physical and non-physical risks and promoting a culture of continuous improvement.
Reg-R06-A06. Monitor, evaluate, and update OHS policies	Set up EU programmes to monitor incidents and health outcomes in automated contexts and use findings to update standards, regulations and guidance.

3.4.3. Actions grouped by category

3.4.3.1. Financing, pilots, and infrastructure deployment

Actions focus on piloting certification and safety frameworks and financing uptake.

Pilot projects should test certification models in real value chains and generate practical guidance. Financing and procurement rules should reward high-quality DPP data, closed-loop recovery and safety frameworks, accelerating circular and safe MaaS deployment.

3.4.3.2. Standardisation of data, cloud, and cybersecurity architectures

Actions build harmonised data frameworks for sustainability, certification, waste and safety.

A unified EU data portal should streamline reporting and transparency. Embedding certification and OHS data into DPPs and standardised formats ensures consistent, secure data exchange. Waste tracking integration supports traceability and circular flows.

3.4.3.3. Data governance, legal alignment and regulatory compliance

Actions promote phased sustainability reporting and consistent governance.

Mandatory reporting should start with high-impact sectors and product groups, supported by robust governance and accreditation mechanisms. DPP obligations should be phased in with clear definitions of scope and data quality. Modernised regulatory surveillance using digital tools will enable continuous oversight.

3.4.3.4. Organisational security and certification

Actions create an integrated MaaS certification model.

Security, environmental, social and economic criteria should be combined in a MaaS certification framework, interoperable with DPPs and ESG reporting. Digital quality passports should provide lifecycle proof of compliance and block non-certified components. Recertification, Zero Waste standards and updated OHS rules will maintain safety and trust.

3.4.3.5. Skills, capacity building and knowledge dissemination

Actions support skills and safety culture.

Training, competence frameworks and guidance should build SME expertise in digital reporting, safe human-robot collaboration and risk management. Participatory risk assessment should address physical and psychosocial impacts. Systematic monitoring of incidents and health outcomes should inform future OHS updates, supported by incentives for training participation.

3.5. Skills and Competences for MaaS

MaaS doesn't remove the humans in manufacturing;
automation and empowerment redefine their role.
Digitisation, data, and AI drive MaaS forward
but the empowered user sets the direction.

3.5.1. Recommendation area overview

The Skills and Competences area addresses how Europe can equip its workforce for MaaS through dedicated competence frameworks, validation and lifelong learning.

Short term, a MaaS competence model and self-assessment tools should define a "must have" skill set for engineers, administrative staff and management, giving a shared language for training and workforce planning. Medium term, personalised, multilingual learning resources should be co-created by SMEs, universities and innovation hubs and delivered via modern platforms that support cross-generational knowledge transfer.

A culture of competence validation and modular certification should allow workers to evidence skills and move easily within European MaaS ecosystems. This keeps skills aligned with automation and data-driven manufacturing and maintains people at the centre of MaaS.

Scope

- A short term goal is to develop a "must have" set of competences for MaaS approaches which can be shared via a network such as the European good practice network
- In the medium term SMEs and universities should create personalised learning materials backed by a competence validation culture and certification framework

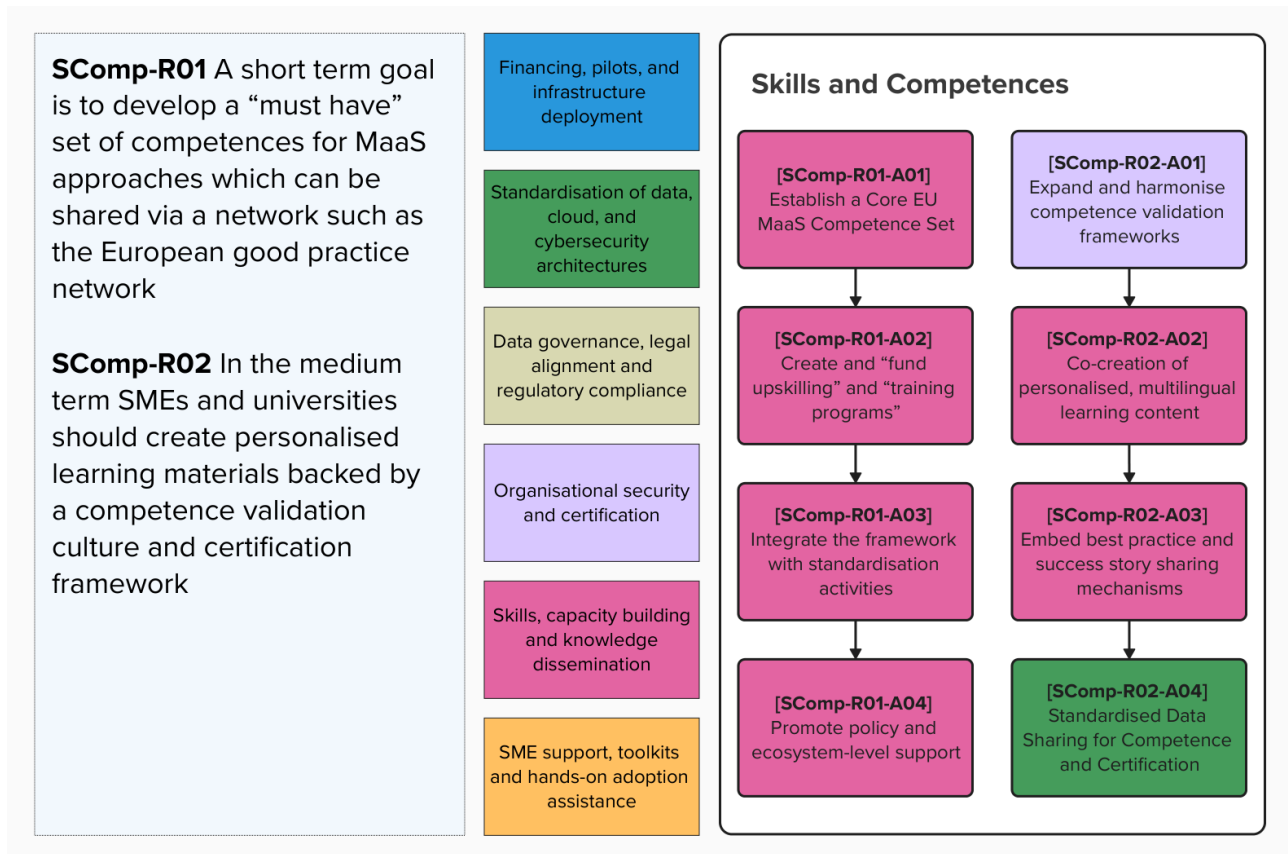## 3.5.2. Recommended actions - Skills and Competences for MaaS

Figure 10. **Skills and Competences for MaaS** recommended actions

3.5.2.1. A short term goal is to develop a "must have" set of competences for MaaS approaches which can be shared via a network such as the European good practice network

Upskilling is required and a dedicated MaaS competence model should be developed, rather than extending existing frameworks like DigComp, EntreComp or GreenComp.

The model should target engineers, administrative staff and management and include a competence self-assessment tool. It should be developed quickly and distributed through European good practice networks to guide training and workforce planning.

Currently there is no EU-wide competence model specific to MaaS, although research and policy discussions highlight the need for skills in federation, digital collaboration, modular production and data-driven manufacturing. A standardised MaaS competence model remains to be established.

Actions under the recommendation

Name of action	Action description
SComp-R01-A01. Establish a Core EU MaaS Competence Set	Convene experts from industry, academia, SDOs and DIHs to define a modular MaaS competence set (technical, digital, management, collaboration) for

Name of action	Action description
	engineers, administrative staff and management and disseminate it via EU good practice networks.
SComp-R01-A02. Create and "fund upskilling" and "training programs"	Launch EU and Member State funding for upskilling and training aligned with the MaaS competence framework, using EDIHs and networks and supporting digital platforms, practical materials and cross-generational knowledge transfer.
SComp-R01-A03. Integrate the framework with standardisation activities	Coordinate with SDOs to align competences with work on interoperability, data spaces and DPPs and support standards and certification for the competence framework and related training.
SComp-R01-A04. Promote policy and ecosystem-level support	Establish an EU observatory and repository for MaaS competences and resources, and provide policy incentives (tax, funding, certification advantages) for organisations adopting and promoting the framework, including integration into education curricula.

3.5.2.2. In the medium term SMEs and universities should create personalised learning materials backed by a competence validation culture and certification framework

A culture of lifelong learning and competence validation is essential for sustainable MaaS growth.

SMEs and universities should co-create targeted, personalised learning resources integrated with competence validation and modular certification schemes. Top-down policy initiatives must be complemented by bottom-up sharing of good practices and success stories, especially via EDIHs in local languages.

Funding at national and EU level should support learning platforms that enable multi-generational knowledge transfer and promote the benefits of automation for job quality and safety. Certification frameworks should make validated skills visible and portable.

Actions under the recommendation

Name of action	Action description
SComp-R02-A01. Expand and harmonise competence validation frameworks	Develop EU-wide MaaS skills and certification frameworks (micro-credentials, modular schemes) with mutual recognition and pilot schemes for emerging roles, integrating workplace-based assignments.
SComp-R02-A02. Co-creation of personalised, multilingual learning content	Co-design adaptive digital learning modules using AI and analytics, produce SME success stories in all official languages and fund large-scale pilots encouraging cross-sector, cross-generational participation.
SComp-R02-A03. Embed best practice and success story sharing mechanisms	Create forums for peer learning where SMEs share automation and MaaS experiences and translate materials for local contexts, using common metrics and templates in EU repositories.
SComp-R02-A04. Standardised Data Sharing for Competence and Certification	Develop interoperable data standards for learning achievements, certifications and outcomes, building on ICT Rolling Plan learner credential work, and align funding and incentives with adoption to ensure portability and comparability.

3.5.3. Actions grouped by category

3.5.3.1. Standardisation of data, cloud, and cybersecurity architectures

Actions develop interoperable data standards for documenting learning, competences and training outcomes. Building on existing European learner credential standards, harmonised data and secure exchange protocols should enable portable, machine-readable records across platforms and borders, supporting worker mobility and transparent recognition of competences across the EU labour market.

3.5.3.2. Organisational security and certification

Actions expand EU-wide competence validation frameworks.

MaaS skills should be defined and certified through modular schemes and micro-credentials, with mutual recognition across Member States. Pilot certifications should address emerging roles (e.g. human-machine collaboration, digital twins, sustainable production) and integrate workplace-based assignments. This provides employers with transparent assurance of skills and workers with clear progression paths.

3.5.3.3. Skills, capacity building and knowledge dissemination

Actions focus on competence models, upskilling and knowledge sharing.

A core MaaS competence set should guide funding for modular training and multilingual resources. Adaptive content, case studies and peer exchanges should support cross-generational learning and demonstrate automation benefits. Monitoring and shared repositories should support consistent, high-quality implementation linked to standards and certification.

4. Stakeholders – summary

During the preparation of this report, a number of stakeholder groups were identified. As the Standardisation Analysis Report clearly showed that many of the initiatives are carried out in cooperation or on the borderline between stakeholder activities, we have grouped the stakeholders as follows in this study. The assignment to groups is the result of the MASTT2040 project research.

4.1. ECDA – European Commission Directorates and Agencies

All EU policy-making, regulatory, oversight, and funding directorates and agencies):

1. DG CONNECT[14] – Digital transformation, data spaces, interoperability, ICT standards,
2. DG GROW[15] – Industrial policy, SME competitiveness, standardisation, manufacturing,
3. DG ENV[16] – Circular economy policy, environmental indicators, ESPR alignment,
4. DG CLIMA[17] – Climate targets, sustainability reporting alignment,
5. DG JUST – Data protection, privacy, consumer safety,
6. DG RTD[18] – Research and innovation funding,
7. DG DEFIS – Supply chain resilience and strategic autonomy,
8. DG TAXUD – Fiscal incentives for green investment,
9. DG EMPL[19] – Skills, training, workforce inclusion,
10. European Data Protection Board (EDPB) – Privacy and consent governance,
11. ENISA – Cybersecurity guidance, certification, NIS2 alignment,
12. ACER / EU-OSHA / JRC / EEA / Eurostat – Sector-specific reg. support, safety, environmental monitoring,
13. Data Protection Officer (DPO[20]),
14. DG CINEA[21] – European Climate, Infrastructure and Environment Executive Agency,
15. Defence Industry and Space (DEFIS[22]),
16. European Innovation Council and Small and Medium-sized Enterprises Executive Agency (EISMEA[23]),
17. European Research Executive Agency (REA[24]),
18. Joint Research Centre (JRC[25]).

---

[14] https://commission.europa.eu/about/departments-and-executive-agencies/communications-networks-content-and-technology_en

[15] https://commission.europa.eu/about/departments-and-executive-agencies/internal-market-industry-entrepreneurship-and-smes_en

[16] https://commission.europa.eu/about/departments-and-executive-agencies/environment_en

[17] https://commission.europa.eu/about/departments-and-executive-agencies/climate-action_en

[18] https://commission.europa.eu/about/departments-and-executive-agencies/research-and-innovation_en

[19] https://commission.europa.eu/about/departments-and-executive-agencies/employment-social-affairs-and-inclusion_en

[20] https://commission.europa.eu/about/departments-and-executive-agencies/data-protection-officer_en

[21] https://commission.europa.eu/about/departments-and-executive-agencies/european-climate-infrastructure-and-environment-executive-agency_en

[22] https://commission.europa.eu/about/departments-and-executive-agencies/defence-industry-and-space_en

[23] https://commission.europa.eu/about/departments-and-executive-agencies/european-innovation-council-and-small-and-medium-sized-enterprises-executive-agency_en

[24] https://commission.europa.eu/about/departments-and-executive-agencies/european-research-executive-agency_en

[25] https://commission.europa.eu/about/departments-and-executive-agencies/joint-research-centre_en

4.2. SDO – Standardisation Development Organisations

All European and international bodies defining technical, semantic, and certification standards:

1. CEN[26], CENELEC[27], ETSI[28] – European harmonised standards,
2. CEN-CENELEC JTC 13, JTC 24, JTC 25 – Data spaces, cybersecurity, DPP,
3. ISO, IEC – Global alignment (LCA, identifiers, digital twins, cybersecurity),
4. ISO/IEC JTC 1 SC 27, TC 307, TC 184, TC 323 – Security, blockchain, manufacturing, circular economy,
5. OPC Foundation – Interoperability and machine connectivity,
6. Weihenstephan Standards Group – Sector-specific data models,
7. SCI4.0 (Standardisation Council Industrie 4.0) – EU–national coordination,
8. EFRAG – Sustainability reporting standards (ESRS),
9. GS1[29], Catena-X – Identification, traceability and DPP schemas,
10. EOTA[30] (European Organisation for Technical Assessment).

4.3. EDIH – European Digital Innovation Hubs[31]

Regional innovation hubs providing SME testbeds, training, support:

1. European Digital Innovation Hubs (EDIHs) – SME onboarding, pilots, eco-design testbeds,
2. Local/regional competence centres contributing to MaaS adoption,
3. DSSC (Data Spaces Support Centre) – Technical support for data spaces and DPP deployment.

4.4. Industry – Industry and SME Associations

Manufacturers, platform providers, integrators, sector alliances:

1. Manufacturing SMEs and OEMs – Implementation and adoption,
2. MaaS platform providers and system integrators,
3. Orgalim – Europe's technology industries,
4. EFFRA – Made in Europe partnership, factories of the future,
5. Digital SME Alliance – SME representation,
6. AIOTI – IoT, edge, digitalisation of manufacturing,
7. European Circular Economy Stakeholder Platform,
8. Sector associations – batteries, electronics, machinery, automotive,
9. Industry consortia – IDSA, Gaia-X, Catena-X, Factory-X.

---

[26] https://www.cencenelec.eu/about-cen/

[27] https://www.cencenelec.eu/about-cenelec/

[28] https://www.etsi.org/

[29] https://www.gs1.org/

[30] https://www.eota.eu

[31] It must be stated that we are not identifying Universities in general as a stakeholders for recommendations for scaling of MaaS. These Universities that we identified as a most relevant for MaaS are involved into EDIHs initiatives. That is why it is so important to cooperate in such networks.

4.5. LegP – Legal, Contract and Ethics Platforms

Legal compliance, contracting, trust frameworks, ethics, ESG:

1. EU Data Act, Data Governance Act platforms – Data sharing and governance rules,
2. European AI Act frameworks – AI governance and risk management,
3. GDPR / data protection compliance bodies,
4. NIS2 implementation platforms – Cybersecurity governance,
5. EU Ecolabel and national ecolabel bodies,
6. European Cooperation for Accreditation (EA) – Cross-border certification integrity,
7. Accredited certification bodies and labs – Conformity, testing, auditing,
8. TIC Council – Testing, inspection and certification Industry.

Sustainability/ESG frameworks – EU Sustainable Finance Platform, GPP Network.

The MASTT2040 project has actively engaged with many relevant stakeholders during the course of the project work as shown in Figure 11 to ensure that they have been fully informed of the standardisation recommendations development. These include relevant DGs, SDOs, Industrial Data Space and Big Data Value organisations as well as actors in Industrie 4.0 and the circular economy. Additionally, relevant EC funded standards projects and organisations with an interest in manufacturing and data standardisation have also been consulted.
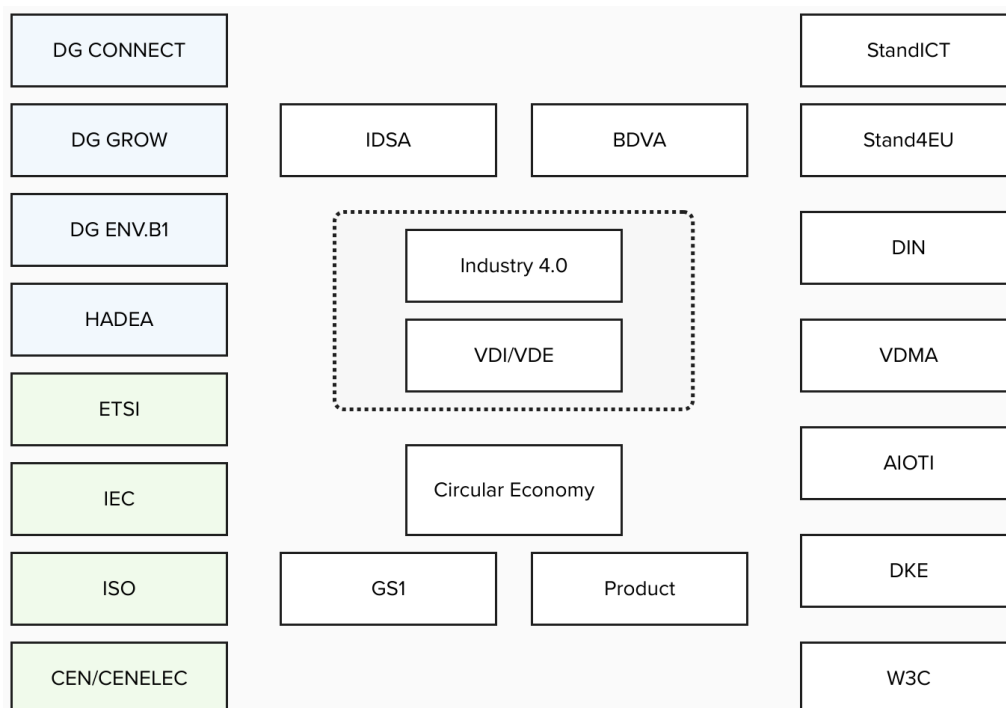
Figure 11. Key Stakeholders for MASTT2040

5. Conclusions

The recommendations presented can be used to guide the European Commission in formation of future policy actions and in promoting industrial data standardisation in support of uptake of MaaS. The work has considered visions for the future of Manufacturing-as-a-Service going to 2040 addressing key European goals with respect to resilience in supply chains, sustainability, circularity and how workers will utilise and integrate with technology in the future. The recommendations cover a number of strategic areas:

- Trusted Data Spaces enabling safe and effective cooperation within Manufacturing-as-a-Service ecosystem,
- Interoperability based on data standardisation and digital tools,
- Circular Economy enabled MaaS,
- Regulation,
- Skills and Competences.

Already there are many initiatives and legislation activities have already been undertaken at the EU level with the common goal to boost Europe's global competitiveness and data sovereignty, e.g. Data Act, AI Act and Cyber Resilience Act. All these initiatives are focused on "the vision of a European single market for data, amongst others by a governance framework for common European data spaces, prioritizing interoperability requirements and standards within and across sectors"[32]. There are, however, still structural challenges within the European standardisation ecosystem which also need addressing in order to facilitate the adoption of these actions. In order to address these a coordinated approach is required that addresses the current high degree of fragmentation in data standardisation activities. There is also a need ensure that actions do not duplicate efforts. A key consideration is that the solutions developed take into account the perspectives of all stakeholders. This needs to particularly address how the proposed solutions may impact European manufacturing stakeholders from large industry to SMEs in individual economic sectors and countries with varying levels of digital maturity.

The EU Data Act[33] which is designed to encourage companies to share maintenance and performance data is seen as positive as data sharing is essential for MaaS. The sharing of data is perceived to be less of a concern for smaller companies who have less data to share. Larger companies have more concerns over sharing data as they see more commercial sensitivity. For tailored products there are concerns that personal data may be shared to multiple entities and this needs to be controlled within a distributed supply chain.

---

[32] COMMISSION IMPLEMENTING DECISION of 1.7.2025 on standardisation request to the European standardisation organisations as regards a European Trusted Data Framework in support of Regulation (EU) 2023/2854 of the European Parliament and of the Council; Brussels, 1.7.2025, C(2025) 4135 final

[33] 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 and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (**Data Act**); creates rules for data access and portability, requiring interoperability standards for connected products and industrial data; The Data Act gives individuals and businesses the right to access the data produced through their utilisation of smart objects, machines and devices

Data sharing is also seen as essential for circularity. A key question that needs answering is what data should be shared? Despite having less data to share, SMEs are scared of breaking regulations and this leads them to be more conservative. The key challenge is in providing best practice/guidelines for data sharing to address this. Stakeholders who can work together on this are the EC and Industry Associations with connections to SMEs. This needs to be done at the local level to provide support and sharing of experiences.