Compliance-by-Design: Validating Decentralised Architectures for Digital Product Passports under the EU Data Governance Act

Christoph Fabianek†, Christoph Klikovits*, Markus Tauber‡,
Belal Abu Naim‡, Michael Boch‡, Martin Benedikt§

*Forschung Burgenland GmbH †Own Your Data ‡Research Studios Austria §Virtual Vehicle

***Abstract*—The Digital Product Passport (DPP) is a cornerstone of the European Union's sustainability and circular economy strategy. While many conceptual frameworks exist, limited work has validated DPP architectures against the regulatory requirements that govern data sharing in the EU. This paper addresses this gap by presenting and assessing a decentralised DPP architecture that integrates data intermediaries, decentralised identity, and cryptographic mechanisms. Using the EU Data Governance Act (DGA) as the primary regulatory lens—complemented by the General Data Protection Regulation (GDPR) and the Ecodesign for Sustainable Products Regulation (ESPR)—we demonstrate how key requirements such as neutrality, structural separation, fair access, registration, and confidentiality are met in practice. Validation is performed through early-stage pilots in the PACE-DPP and USEFLEDS projects, which provide empirical evidence of compliance-by-design approaches. Findings highlight that decentralised governance and regulated data intermediaries not only enhance interoperability and trust but also operationalize regulatory mandates, creating a robust foundation for legally compliant, scalable, and sustainable DPP ecosystems.**

***Index Terms*—Digital Product Passport (DPP), Battery Passport, Data Intermediaries, Data Governance Act (DGA), Decentralised Governance, Data Sovereignty, Data Security**

I. Introduction

In the context of the European Union's sustainability strategy, the Digital Product Passport (DPP) has emerged as a cornerstone to advance circular economies and improve transparency across supply chains. The DPP provides a foundation for Industry 4.0 use cases, where digital infrastructures support sustainable product lifecycles by enabling electronic components and systems to be reused or recycled,. However, realizing this vision requires more than technical innovation: it demands governance frameworks that are compliant with European regulations, most notably the Data Governance Act (DGA), as well as related instruments such as the General Data Protection Regulation (GDPR) and the Ecodesign for Sustainable Products Regulation (ESPR).These factors highlight the importance of designing practical implementations that integrate technology with compliance and stakeholder collaboration [1].

This project was funded in the program "Leitprojekt Daten-Service-Ökosystem für die Energiewende 2022" by FFG and BMK under grant number 905128.

A central challenge is ensuring secure, efficient, and transparent data exchange between diverse stakeholders, including manufacturers, regulators, and service providers. The DPP aims to act as a shared infrastructure that prevents the concentration of data within proprietary silos while promoting equitable access and collaboration across industries. Given the sensitivity of the information involved—from intellectual property to compliance-critical data—any DPP implementation must safeguard privacy, sovereignty, and adherence to regulatory requirements. Without compliance, trust in the system and its long-term sustainability would be severely undermined [2].

Existing research on DPPs has largely focused on conceptual frameworks and standardization efforts but has not sufficiently addressed how decentralised, industry-driven governance can be operationalized in a way that demonstrably meets legal obligations [3]. Without explicit links between technical mechanisms and compliance requirements, there is a risk that data-sharing infrastructures will be captured by dominant players, leading to asymmetric benefits and reduced participation from smaller stakeholders. Decentralised governance approaches—using cryptographic proofs, verifiable credentials, and decentralised identity management—offer promising tools to support sovereignty and trust in data ecosystems. Yet, their effectiveness in fulfilling concrete regulatory obligations remains insufficiently validated.

This paper proposes and evaluates a DPP architecture that integrates data intermediaries with decentralised governance mechanisms in line with the requirements of the DGA [4] to address the gap. This approach enhances transparency, trust, and resilience within DPP ecosystems by combining distributed decision-making with compliance-by-design principles. The architecture is validated through early findings from two large-scale projects, USEFLEDS and PACE-DPP, which illustrate how technical features such as decentralised identifiers (DIDs), verifiable credentials (VCs), and zero-knowledge proofs (ZKPs) can be mapped to regulatory requirements. This paper contributes a practical framework for ensuring that DPP ecosystems are not only technically robust but also legally compliant and trustworthy.

The remainder of this paper is structured as follows. Sec-

978-3-903176-75-1 ©2025 IFIP

tion II discusses the background and related work, exemplified by the Battery Passport, which is widely acknowledged as a reference initiative for the DPP, and highlights existing approaches and gaps.Section III presents the proposed architecture and outlines its technical and decentralised governance aspects and its compliance assessment in Section VI. Finally, Section V and Section VII present the assumptions and limitations of the study, conclude the paper, and provide insights into future research paths.

II. Related Work

The concept of Digital Product Passports (DPPs) has been widely explored in recent years, with a particular focus on their potential to enhance sustainability and enable circular economies [5]. For batteries, DPPs are critical for addressing environmental concerns and supporting transparent, efficient lifecycle management. Existing research and policy documents provide a comprehensive foundation for understanding the challenges and opportunities of implementing DPPs [6].

The World Economic Forum highlights the Digital Battery Passport as an enabler for sustainable and circular battery management, emphasizing its role in creating transparency and trust in battery supply chains. Similarly, the European Commission and the Council of the European Union provide a regulatory framework for ecodesign requirements for sustainable products, including batteries. These regulations set the stage for integrating DPPs into European sustainability efforts but leave open questions about practical implementation [7].

King *et al.* [8] propose a universal definition of a Digital Product Passport Ecosystem (DPPE), detailing the necessary capabilities, stakeholder requirements, and concerns. Their work underscores the importance of governance and interoperability within DPP systems, aligning with regulatory requirements while addressing stakeholder expectations.

Technical challenges in DPP implementation include the standardization of data attributes and ensuring interoperability across platforms. The Battery Pass Consortium offers a comprehensive list of data attributes essential for DPPs, developed in collaboration with the Global Battery Alliance. However, their work primarily focuses on data collection and does not address the integration of governance frameworks into technical architectures [9].

Weng *et al.* [10] discuss the role of battery passports in promoting electric vehicle (EV) resale and repurposing, identifying key challenges such as data sharing across competitive stakeholders and the need for secure systems. Their findings support the need for architectures like data intermediaries to ensure trust and compliance in DPP ecosystems.

Kotak *et al.* [11] analyze the end-of-life management of EV batteries, comparing reuse and recycling scenarios. They argue that DPPs can facilitate decision-making by providing reliable data on battery conditions and history. However, their work does not explore how DPPs can be practically implemented in a secure and compliant manner.

The role of governance in DPPs is critical for fostering trust and ensuring compliance with regulatory standards. Adisorn *et al.* [12] emphasize the importance of aligning DPPs with circular economy goals, focusing on transparency and sustainability. Similarly, Basel Action Network (BAN) and Langley *et al.* [13] identified gaps in the circular economy, such as WEEE leakage from Europe, highlighting the need for robust tracking mechanisms like DPPs [14].

Beyond traditional governance models, decentralised governance has emerged as a key approach to addressing trust and data sovereignty challenges in digital ecosystems. Initiatives such as Gaia-X propose a federated data infrastructure where participants retain control over their data while ensuring interoperability and regulatory compliance [15]. Ocean Protocol introduces a decentralised data marketplace leveraging blockchain and smart contracts to enable fair and secure data exchange while preventing data monopolization [16]. Furthermore, SOLID Pods, introduced by Tim Berners-Lee, advocate for personal data stores that empower individuals with control over their data while enabling decentralised and consent-based data-sharing models [17].

While these works provide valuable insights, practical solutions for integrating decentralised governance frameworks with technical architectures are still under development. This area presents opportunities for further exploration, particularly in discussions around the DGA and the implementation of secure data-sharing mechanisms.

The approach proposed in this paper aims to build on prior work by integrating data intermediaries into the data processing layer of the Digital Battery Passport. While previous studies have provided valuable insights, they often emphasize abstract frameworks or specific aspects of DPP implementation. This work seeks to address the intersection of technical and governance requirements by leveraging data intermediaries to enable secure, transparent, and compliant data exchange in alignment with EU regulations.

III. Architecture

A Digital Product Passport (DPP) ecosystem involves key stakeholders collaborating throughout the product lifecycle:

- The Government defines the regulatory framework, ensuring compliance and standardization through legislation and audits, shaping the roles of Data Providers and Service Providers.
- Data Providers supply essential product lifecycle information, which the data intermediary manages and mediates, ensuring that it is structured, catalogued, and made securely available to authorized stakeholders. This data enables Service Providers to deliver services such as analytics, reporting, or recycling strategies.
- Ecosystem actors, such as supply chain participants, auditors, recyclers, and end users, use the intermediary catalog to access data and services, supporting compliance and sustainability.

The proposed architecture introduces a multi-layered governance model that combines Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and federated access control. This model ensures that manufacturers, regulators, and service

providers can engage in a trustless exchange of data while maintaining sovereignty over their respective datasets. Beyond enabling secure and transparent data flows, the integration of these mechanisms operationalizes regulatory requirements by design: neutrality is embedded through structural separation of roles, fair access is enforced via standardized credentialing and permissioning, and confidentiality is safeguarded through cryptographic proofs and selective disclosure. By aligning technical building blocks directly with obligations under the Data Governance Act (DGA), the GDPR, and the ESPR, the architecture advances a Compliance-by-Design paradigm, where conformity with European regulatory frameworks is not an afterthought but a core property of the system itself.
The core components include:

- Data Intermediary Layer: A federated infrastructure that enables permissioned data exchange through standardized APIs, compliant with the EU Data Governance Act (DGA).
- Identity and Access Management: Verifiable identity structures based on DID and EUDI wallet integrations for controlled data access.
- Security Mechanisms: Integration of cryptographic proof-based access verification, ensuring secure interactions between data providers and consumers.

A high-level architecture diagram illustrating these interactions is provided in figure 1.

The Data Intermediary serves as a regulated facilitator, organizing, and granting access to information through its data and service catalog.

Figure 2 illustrates how the Digital Product Passport (DPP) can be modeled through the interaction of stakeholders, data flow, and the legal framework established by the government. It highlights key aspects of **Process**, **Data Exchange**, and **Governance** within the data ecosystem, showcasing how legislation, data collection, regulated data sharing, service provision, and identity-based governance work together to ensure privacy, compliance, secure service delivery, and effective implementation of the DPP.

At the core of this system is the **Data Intermediary**, which acts as a platform that collects, stores, and facilitates the exchange of data among stakeholders, service providers, and end-users. In our proposed design the data intermediary uses decentralised technologies to provided a trustless architecure that ensures data sovereignty, enhances privacy through cryptographic mechanisms, and enables secure peer-to-peer transactions without reliance on a central authority. By leveraging decentralised identifiers (DIDs), verifiable credentials (VCs), zero-knowledge proofs (ZKPs), and the Semantic Overlay Architecture (SOyA [18]), our system enforces transparent governance, automates compliance, and mitigates risks associated with data monopolies and unauthorized access.

The process begins with the **Government** defining data models that specify the attributes and constraints required for the DPP. These models are authored with SOyA and describe the format, validation rules, as well as capturing mechanisms (forms) to establish a uniform structure for data collection and exchange. The government also regulates services and processes related to the DPP and specifies access control mechanisms (enforced through DIDs), ensuring that sensitive data is securely managed. This creates a foundation for all subsequent actions.

Upstream Organisations, such as manufacturers and suppliers, are responsible for collecting data throughout the supply chain. This includes essential information on materials, environmental impact, and product lifecycle details. Once gathered, the data—along with its associated metadata—is submitted to the data intermediary. The intermediary organizes and securely stores this information, recording relevant metadata, such as ownership, using DIDs. This ensures that authorized stakeholders can access the data efficiently and securely.

Service Providers interact with the data intermediary to offer value-added services, including the creation and enhancement of Digital Product Passports (DPPs), data processing, and the provision of analytical tools. To facilitate secure and transparent data exchange, Verifiable Credentials (VCs) are used to document consent, ensuring that data is shared only with authorized entities under predefined conditions. This guarantees compliance with data governance policies while preserving privacy and trust. Service providers then transform the collected data into actionable insights or products that support the goals of the DPP, such as sustainability, resource efficiency, and fostering a circular economy.

End-users, such as auditors, recyclers, or organizations involved in circular economy initiatives, access Digital Product Passport (DPP) data via the audited data intermediary, which ensures long-term availability. Every data access request is logged immutably, creating a tamper-proof audit trail that documents when, by whom, and for what purpose data was accessed. This ensures transparency, accountability, and compliance with data governance policies. End-users can query the data for specific purposes, such as compliance checks, resource recovery, or product recycling. Access is strictly governed by privacy regulations and compliance standards to ensure that sensitive information is handled securely and appropriately.

The data intermediary manages the identity using decentralized identifiers (DIDs), ensuring secure and verifiable authentication for all participants. Each organization or individual is assigned a DID, which is cryptographically linked to a government-issued identity, providing a trusted foundation for interactions. The current implementation also supports the OpenID for Verifiable Credentials (OID4VC) standard, enabling seamless integration with upcoming European Digital Identity (EUDI) wallets. This ensures compatibility with evolving regulatory frameworks while maintaining decentralization, security, and interoperability across identity ecosystems.

Data disclosure between participants must balance transparency with confidentiality, ensuring that only relevant information is shared without exposing business-critical or internal data. The data intermediary can facilitate this using zero knowledge proofs (ZKPs), allowing participants to ver-

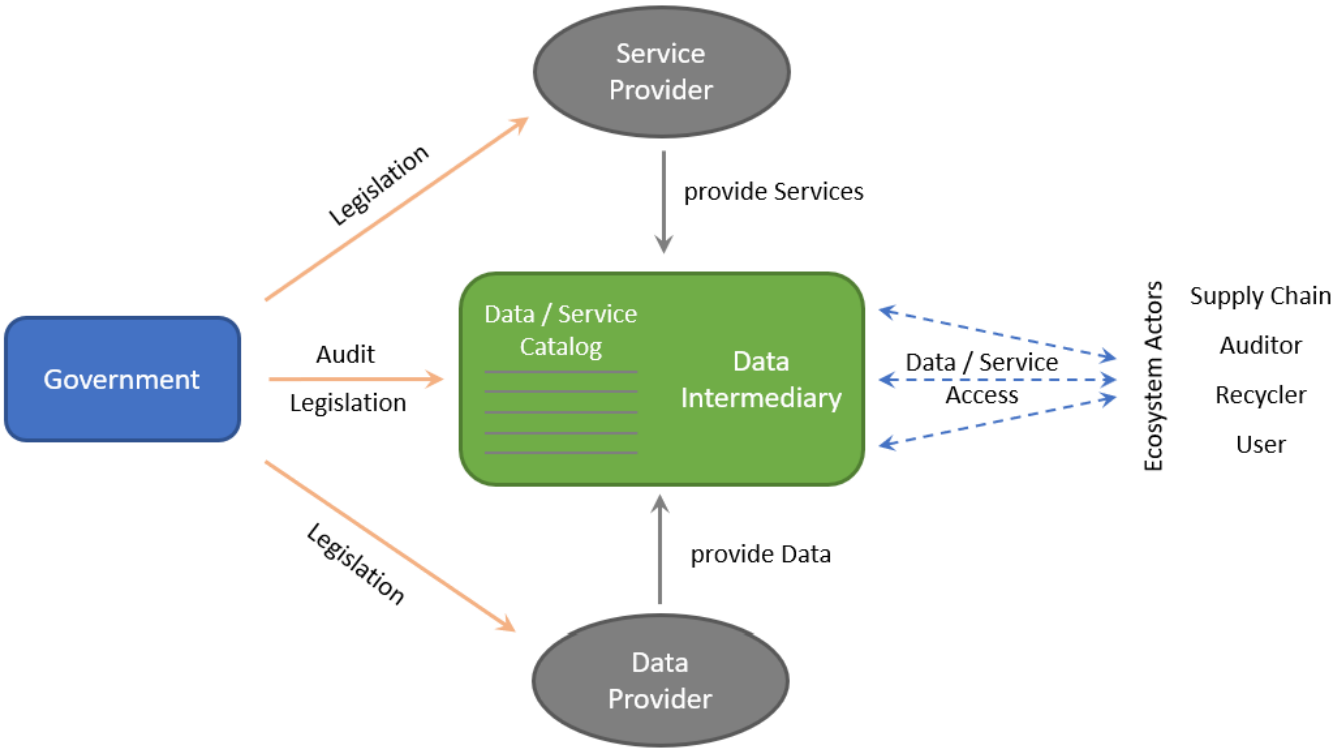

Fig. 1. Stakeholders in the DPP ecosystem

ify specific claims, such as compliance with regulations or material origin, without revealing underlying sensitive data. By leveraging ZKPs, the intermediary ensures that trust is established while minimizing data exposure, enabling secure and selective information sharing between stakeholders in a privacy-preserving manner.

IV. Proof of Concept and Validation

To validate the proposed approach, we conducted an early-stage implementation within the USEFLEDS and PACE-DPP projects. A federated intermediary infrastructure was tested with real-world data-sharing scenarios, focusing on regulatory compliance, interoperability, and security. Key findings include:

The integration of DIDs and VCs enabled fine-grained access control without requiring a centralized authority. The API-based data exchange layer was successfully mapped to existing industrial interoperability frameworks (e.g., GS1, ISO 14083). Early stage trials highlighted adoption barriers among small and medium enterprises, particularly in terms of cost-efficiency and standardization efforts.

These insights inform future scalability improvements and further pilot implementations.

V. Assumptions and Limitations

The proposed DPP architecture relies on several key assumptions. It assumes that all stakeholders—manufacturers, suppliers, service providers, and regulators—will actively collaborate within a shared governance and technical framework, supported by transparent participation and mutual trust. It also assumes alignment with EU regulations such as the DGA, ESPR, and GDPR, ensuring legal compliance. Further, the approach also assumes that upstream stakeholders, such as manufacturers and suppliers, will provide accurate, comprehensive, and timely data about product lifecycles. Without high-quality data, the utility of the DPP could be significantly reduced. In addition, the adoption of standardized data attributes, as outlined by initiatives like the Battery Pass Consortium, is crucial to achieving interoperability across platforms. Lastly, it is assumed that the technological infrastructure, including secure data exchange mechanisms and identity management systems, is sufficiently mature to meet the demands of the DPP ecosystem.

Despite these foundations, several limitations remain. Interoperability challenges persist across different DID methods, and the Verifiable Credentials (VC) model is still evolving, which may hinder seamless cross-platform use. Zero-Knowledge Proofs (ZKPs) provide strong privacy guarantees but remain computationally expensive, limiting real-time scalability. In addition, high initial costs and technical complexity can deter SMEs from adopting, while handling sensitive or competitive information between multiple stakeholders raises trust concerns. Scalability has yet to be validated in large-scale deployments, where higher data volumes and user diversity may expose performance bottlenecks. Finally, stakeholder resistance—driven by perceived risks, workflow disruptions, or unclear benefits—could slow adoption, underscoring the need

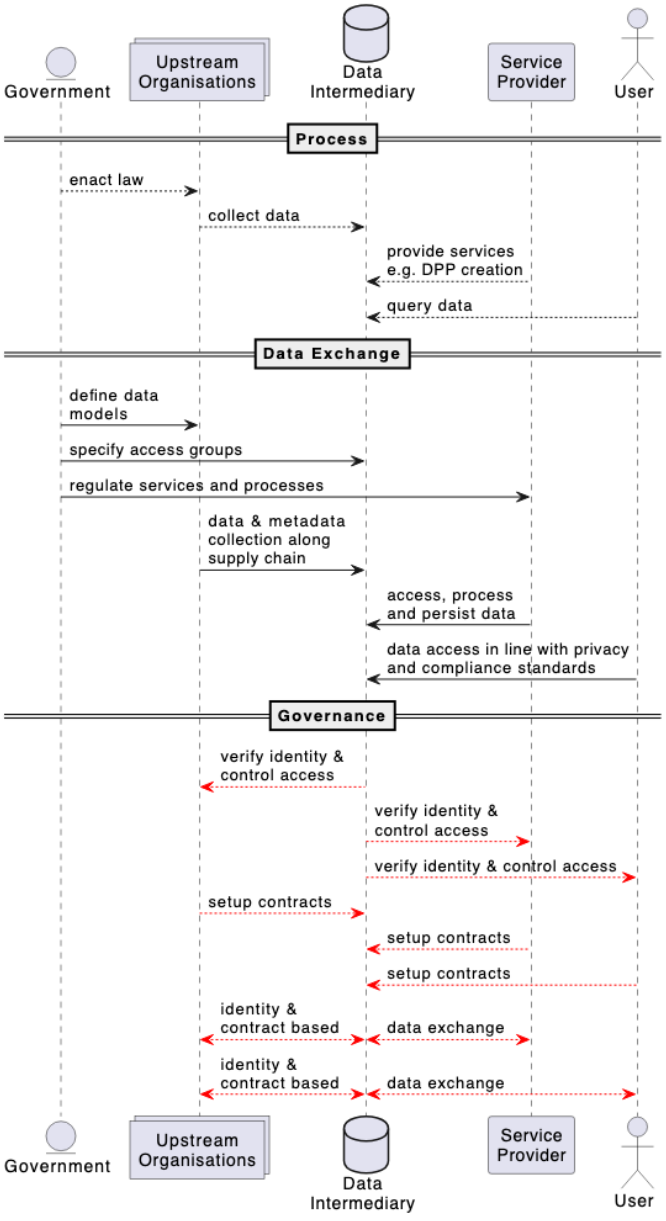

Fig. 2. Sequence diagram interactions within the DPP

for outreach, standardization, and user-friendly tools.

VI. Regulatory Requirements and Assessment

An essential part in the DPP ecosystem is the sharing of data. This requires compliance with the DGA. The DGA introduces a regulatory framework for data intermediation services to facilitate secure and neutral data sharing between entities. These services act as intermediaries, connecting data holders with data users while ensuring compliance with European data protection standards. Key Features of Data Intermediation Services under the DGA:

- Neutrality and Conflict of Interest Avoidance:
  - Requirement: Providers must operate impartially, avoiding any conflicts of interest. They are prohibited from using the data they intermediate for their own purposes, such as developing new products or services based on that data. This ensures that the data-sharing environment remains trustworthy and that intermediaries do not exploit the data for a competitive advantage.
  - Assessment: This requirement is addressed through the establishment of a dedicated legal entity tasked specifically with operating the data intermediary. Furthermore, implementing the data intermediation service using a decentralized architecture is crucial, as it enhances transparency and allows the intermediary to function as a trustless entity within the broader ecosystem.
- Structural Separation:
  - Requirement: To maintain neutrality, there must be a clear legal separation between data intermediation services and any other services offered by the provider. This structural separation prevents potential conflicts between the interests of the intermediation service and other business areas of the provider.
  - Assessment: A decentralised architecture minimises central control risks by distributing governance and operational authority, thereby preventing single points of failure or misuse. Additionally, it improves auditability and compliance through inherent transparency and verifiable record-keeping, simplifying continuous regulatory oversight. Lastly, decentralisation enhances resilience against legal and regulatory challenges by embedding structural compliance directly into its technical framework.
- Fair and Non-Discriminatory Access:
  - Requirement: Providers are required to offer their services under fair, transparent, and non-discriminatory terms. This includes equitable pricing structures and ensuring that no data holder or user is unfairly disadvantaged, promoting a level playing field for all participants.
  - Assessment: A decentralised architecture effectively prevents market dominance by distributing control, ensuring that no single entity can disproportionately influence data access or terms. This approach fosters neutral and unbiased governance, providing an impartial platform for all participants. Consequently, smaller or less influential entities are empowered, enjoying equitable participation opportunities and encouraging broader inclusivity and innovation within the ecosystem.
- Registration and Oversight:
  - Requirement: Data intermediation service providers must register with designated national authorities. This registration process ensures that providers meet the necessary requirements and allows for ongoing oversight to maintain compliance with the DGA's provisions.

  - Assessment: A decentralised architecture significantly enhances transparency for regulatory oversight by providing tamper-evident, openly verifiable records of provider activities, facilitating continuous compliance monitoring by authorities. Additionally, the inherent openness and distributed governance improve trust and accountability among all stakeholders, promoting confidence that data intermediation services consistently adhere to regulatory standards.
- Security and Confidentiality Measures:
  - Requirement: Providers are obligated to implement robust measures to protect the data they handle, ensuring confidentiality and preventing unauthorized access or breaches. This includes technical and organizational safeguards aligned with data protection regulations.
  - Assessment: A decentralised architecture reduces the risk of centralized breaches by distributing data storage and management across multiple nodes, eliminating single points of vulnerability. This approach enhances data control and privacy, enabling data owners to directly manage access through cryptographic methods and transparent authorization. Additionally, decentralisation improves resilience and availability, ensuring continuous data protection and service reliability even in the face of disruptions or targeted attacks.

VII. Conclusion, Summary of Contributions, and Future Work

This work demonstrates that Digital Product Passport ecosystems can be designed and validated with regulatory compliance at their core. By embedding decentralised governance and data intermediaries, the proposed architecture aligns with the DGA's neutrality, fairness, and security principles while enhancing transparency and trust. The pilot results confirm the feasibility of a compliance-by-design approach, although challenges remain in terms of interoperability, cost efficiency for SMEs, and scalability. Future research will expand validation across industries and refine standards, ensuring that DPPs evolve into legally robust, decentralised enablers of the circular economy.

This paper makes three key contributions:

- Compliance-by-Design Architecture – We propose a decentralised DPP architecture that integrates data intermediaries, DIDs, VCs, and ZKPs, explicitly mapped to regulatory requirements under the DGA, GDPR, and ESPR.
- Regulatory Validation Framework – We assess how the architecture satisfies specific legal obligations, including neutrality, structural separation, fair access, oversight, and confidentiality.
- Empirical Validation – Using findings from the PACE-DPP and USEFLEDS projects, we provide early evidence that compliance principles can be operationalized in real-world data-sharing scenarios.

Future work will expand validation of the DPP architecture in large-scale, multi-domain pilots to assess scalability, performance, and adoption. Efforts will focus on improving data interoperability through advanced standards, creating SME-friendly tools to lower adoption barriers, and establishing a policy feedback loop so implementation insights inform evolving regulations. These steps aim to strengthen DPPs as scalable, inclusive, and sustainable enablers of the circular economy.

References

[1] Ducuing, C., & Reich, R. H. (2023). Data governance: Digital product passports as a case study. Competition and Regulation in Network Industries, 24(1), 3-23.

[2] Schneider, I. (2023). Digital Sovereignty and Governance in the Data Economy: Data Trusteeship Instead of Property Rights on Data. In A Critical Mind: Hanns Ullrich's Footprint in Internal Market Law, Antitrust and Intellectual Property (pp. 369-406). Berlin, Heidelberg: Springer Berlin Heidelberg.

[3] Walden, Joerg & Steinbrecher, Angelika & Marinkovic, Maroye. (2021). Digital Product Passports as Enabler of the Circular Economy. Chemie Ingenieur Technik. 93. 10.1002/cite.202100121 .

[4] European Data Governance Act — Shaping Europe's digital future from https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

[5] Psarommatis, F., & May, G. (2024). Digital Product Passport: A Pathway to Circularity and Sustainability in Modern Manufacturing. Sustainability, 16(1), 396. https://doi.org/10.3390/su16010396

[6] Jansen, M., Meisen, T., Plociennik, C., Berg, H., Pomp, A., & Windholz, W. (2023). Stop Guessing in the Dark: Identified Requirements for Digital Product Passport Systems. Syst., 11, 123.

[7] Unlocking the Value of the EU Battery Passport: An exploratory assessment of economic, environmental and social benefits. Retrieved from https://thebatterypass.eu/assets/images/value-assessment/pdf/2024_BatteryPassport_Value_Assessment.pdf

[8] King, M. R., Timms, P. D., & Mountney, S. (2023). A proposed universal definition of a Digital Product Passport Ecosystem (DPPE): Worldviews, discrete capabilities, stakeholder requirements and concerns. *Journal of Cleaner Production, 384*, 135538.

[9] The Battery Pass Long List from https://thebatterypass.eu/assets/images/content-guidance/pdf/2023_Battery_Passport_Data_Attributes.xlsx

[10] Weng, A., Dufek, E. & Stefanopoulou, A. (2023). Battery passports for promoting electric vehicle resale and repurposing. Joule, 7(5), 837–842. https://doi.org/10.1016/j.joule.2023.04.002

[11] Kotak, Y., Marchante Fernández, C., Canals Casals, L., Kotak, B. S., Koch, D., Geisbauer, C., ... & Schweiger, H. G. (2021). End of electric vehicle batteries: Reuse vs. recycle. Energies, 14(8), 2217.

[12] Adisorn, T., Tholen, L., & Götz, T. (2021). Towards a digital product passport fit for contributing to a circular economy. Energies, 14(8), 2289.

[13] Holes in the Circular Economy - WEEE Leakage from Europe from https://wiki.ban.org/images/f/f4/Holes_in_the_Circular_Economy-_WEEE_Leakage_from_Europe.pdf.

[14] Langley, D. J., Rosca, E., Angelopoulos, M., Kamminga, O., & Hooijer, C. (2023). Orchestrating a smart circular economy: Guiding principles for digital product passports. Journal of Business Research, 169, 114259.

[15] Otto, B. (2022). A federated infrastructure for European data spaces. Communications of the ACM, 65(4), 44-45.

[16] Honkanen, P., Nylund, M., & Westerlund, M. (2021). Organizational Building Blocks for Blockchain Governance: A Survey of 241 Blockchain White Papers. Frontiers in Blockchain Vol. 4. https://doi.org/10.3389/fbloc.2021.613115

[17] Sambra, A.V., Mansour, E., Hawke, S., Zereba, M., Greco, N., Ghanem, A., Zagidulin, D., Aboulnaga, A., & Berners-Lee, T. (2016). Solid : A Platform for Decentralized Social Applications Based on Linked Data.

[18] Ekaputra, F. J., Fabianek, C., Unterholzer G., & Gringinger E. (2023) The Semantic Overlay Architecture for Data Interoperability and Exchange. IEEE International Conference on Data and Software Engineering (ICoDSE), pp. 232-237, doi: 10.1109/ICoDSE59534.2023.10291689 .