CONSULTATION RESPONSE

Draft Commission Implementing Regulation Laying Down the Implementation Arrangements for the Digital Product Passport Registry

Document Reference: Ref. Ares(2026)4424976

Feedback submitted by the European Pirate Party (PPEU) | May 2026

The European Pirate Party is a pan-European political party representing Pirate Parties across EU Member States. Our movement is rooted in the defence of digital rights, civil liberties, and democratic participation. We advocate for civil rights, transparency, and the protection of fundamental freedoms in the digital age, and we view digital infrastructure as a common good that must serve all citizens. Our manifesto commits us to privacy by design, free and open-source software, transparent and accountable governance of public digital systems, and the protection of fundamental rights in the digital sphere.

Why We Are Responding

The draft Implementing Regulation for the Digital Product Passport Registry establishes a large-scale data governance infrastructure with significant implications for privacy, accountability, and fundamental rights. While the Registry is presented as a technical support system for sustainability and product traceability under Regulation (EU) 2024/1781, the draft in practice establishes a centralised identity and logging infrastructure that processes extensive amounts of personal data across the Union. The Commission's proposal therefore deserves close scrutiny under both the GDPR and Regulation (EU) 2018/1725.

We are responding because the structural choices embedded in this Implementing Regulation, on identity verification, data retention, log systems, semantic governance, and access control, will shape the Registry's impact on privacy, market access, and civic accountability for years after it goes live. We support the DPP system and its sustainability objectives. Our critique is about how the Registry is governed and whether its design is consistent with the fundamental rights obligations that bind the Commission as data controller.

---

1. Data Protection and Privacy Architecture

The draft correctly designates the Commission as controller for Registry data processing under Regulation (EU) 2018/1725, particularly in Articles 18 and 21. However, the Regulation does not sufficiently demonstrate compliance with the core principles of data minimisation, purpose limitation, proportionality, and privacy by design required under Article 4(1)(c) of Regulation (EU) 2018/1725 and Article 5(1)(c) GDPR. The current approach appears driven by operational convenience and maximal traceability rather than strict necessity.

1.1 Article 18: Scope and Proportionality of Personal Data Collected

Article 18 is particularly problematic in this regard. The list of personal data categories to be stored in the Registry is exceptionally broad. It includes names, postal addresses, email addresses, authentication credentials, document metadata, passport numbers, national identity card numbers, civil registry numbers, tax identification numbers, and third-country identifiers. The draft does not explain why many of these identifiers are necessary for the functioning of the Registry, nor does it distinguish between data required for one-time verification and data requiring long-term storage.

This is difficult to reconcile with the principle of data minimisation under Article 5(1)(c) GDPR and Article 4(1)(c) of Regulation (EU) 2018/1725, both of which require personal data to be adequate, relevant, and limited to what is necessary for the stated purpose. The systematic storage of civil registry numbers, passport numbers, and tax identification numbers appears disproportionate for a system whose primary purpose is product registration and traceability rather than law enforcement or border management. The draft also allows storage of metadata embedded in uploaded documents where such metadata contributes to identification or verification. This wording is vague and potentially overbroad: metadata often contains hidden or incidental personal information unrelated to verification, including device identifiers, location data, timestamps, or internal organisational information.

1.2 The Log System and Behavioural Profiling Risk

Article 14 requires the Commission to maintain a complete, accurate, and reliable audit trail covering authentication attempts, administrative actions, modifications, and data exchanges. While cybersecurity and accountability objectives are legitimate, the retention periods appear insufficiently justified. Administrative and data exchange logs may be retained for five years, while modification logs are retained for the full duration of the registration. Given that registration data itself may remain available for ten years under Article 10(3), this creates the possibility of decade-long behavioural records covering user interactions with the Registry.

The proposal does not adequately distinguish between logs that are strictly necessary for incident detection and logs that effectively enable long-term monitoring of user behaviour. This distinction matters because logging systems can easily become tools for secondary surveillance purposes, particularly when they record unsuccessful access attempts, permission changes, and administrative actions linked to identifiable individuals. The draft refers repeatedly to accountability and traceability but provides little explanation of proportionality safeguards, deletion criteria, or access limitations. Nor does it define what constitutes relevant logs when national authorities request access under Article 14(4).

1.3 Data Subject Rights

Apart from a narrow right to request deletion of a Registry account under Article 10(4), the draft contains almost no operative provisions concerning rights of access, rectification, restriction of processing, or objection. These rights are not optional under Regulation (EU) 2018/1725. Chapter III of that Regulation establishes enforceable obligations on Union institutions acting as controllers, including transparent procedures for exercising rights and clear information duties toward data subjects. Merely stating that personal data will be processed in accordance with Regulation (EU) 2018/1725 is not sufficient where the Registry

itself creates new large-scale processing operations with extensive cross-border access and long retention periods.

1.4 Controller Designation and Split Accountability

Article 21 designates the Commission as controller of Registry data, while Article 22(3) designates Member States as controllers for their own processing activities under the GDPR. This division may appear straightforward in theory, but the Regulation does not address situations where the Commission shares log data or Registry information with national authorities for enforcement purposes under Article 21(3). In practice, such processing operations are likely to involve overlapping purposes and shared decision-making, particularly in market surveillance or customs investigations. The draft does not clarify whether certain enforcement-related processing operations may give rise to joint controllership scenarios. This creates legal uncertainty for data subjects seeking to exercise their rights or identify responsibility for unlawful processing.

1.5 Third-Country Operators: A Structural Gap

Articles 4 and 5 require non-EU economic operators and value chain actors to rely on qualified electronic signatures, seals, or electronic attestations of attributes issued under Union law. The proposal does not explain how operators established in jurisdictions without eIDAS equivalence arrangements are expected to comply. In practice, this may either exclude legitimate non-EU actors from the Registry or encourage inconsistent enforcement of identity verification obligations. This issue is not merely technical. It directly affects fairness, accessibility, and the inclusiveness of circular economy participation. Smaller repair, refurbishment, and recycling actors outside the Union may face disproportionate barriers to participation despite contributing to sustainability objectives under ESPR.

We call on the Commission to:

- Require a formal data minimisation assessment before the Registry becomes operational, with consultation of the European Data Protection Supervisor, requiring the Commission to justify each personal data category in Article 18 as strictly necessary and whether less intrusive alternatives exist.
- Insert operative provisions on data subject rights (access, rectification, restriction, objection) directly into the Regulation, with timelines, contact points, and rules governing access to logs containing personal data.
- Require joint-controller agreements or equivalent arrangements under Article 28 of Regulation (EU) 2018/1725 where Registry data is shared with national authorities for enforcement purposes.
- Establish a transparent equivalence mechanism for third-country trust service frameworks and provide alternative verification pathways for operators in jurisdictions without formal eIDAS equivalence.
- Require deletion of sensitive identifiers such as passport numbers and civil registry numbers once verification has been successfully completed, unless clear legal necessity for continued storage can be demonstrated.

2. Digital Identity, Verification, and the Decentralised Architecture

The Registry's identity and verification architecture raises concerns that go beyond data protection compliance. By gating market access on eIDAS-compliant digital identity infrastructure, concentrating semantic control in the Commission, and failing to require open licensing or independent audit of the Registry's technical components, the draft creates structural risks of incumbency lock-in, surveillance, and proprietary dependency that are inconsistent with the EU's own open infrastructure commitments.

2.1 Mandatory eIDAS Verification Against the Voluntary-Use Principle

Access to the Registry depends entirely on eIDAS identity tools: economic operators and every other actor obtain verified status only through a qualified electronic signature or an electronic attestation of attributes under Regulation (EU) No 910/2014 (Articles 4 and 5). The draft operationalises the broader eIDAS 2 trust and identity ecosystem within a mandatory commercial compliance environment. Yet Regulation (EU) 2024/1183 (eIDAS 2) holds that the wallet is voluntary and free for individuals and businesses, and that users must not be hindered in accessing services for declining to use it. Conditioning Registry participation on eIDAS-compliant verification mechanisms may create de facto dependence on the Union trust-service ecosystem for market participation, particularly for SMEs and non-EU actors, and therefore warrants closer proportionality and accessibility assessment

This mirrors concerns already raised in our earlier submissions on the Digital Identity Wallet and QEAAs: identity infrastructure becoming a gatekeeper rather than a tool.

2.2 Verified Status as a Single Point of Market-Access Failure

Verified status expires when an operator's electronic identification means expire or after three years, whichever comes first; thereafter the operator cannot register new digital product passports (Articles 4(4) and 5(4)). Because DPP registration is a legal precondition for placing products on the market under ESPR delegated acts, expiration of verified status is effectively a market-access suspension. The draft provides no grace period, no notification requirement, and no appeal mechanism. For smaller operators with limited administrative capacity, this is disproportionate. A system that can suspend market access through an administrative lapse, without procedural safeguards, is incompatible with the principles of legal certainty and proportionality.

2.3 The Log System as Surveillance Infrastructure

Complementing the data protection concerns in Section 1, Article 14's logging architecture warrants analysis from a surveillance perspective. The logs, read together, enable reconstruction of which operators accessed which parts of the Registry, when, from where, and what they changed. While audit trails serve legitimate accountability functions, Article 14(5) requires technical and organisational measures to ensure the immutability and confidentiality of the logs, but addresses only the security of logs as such. The provision says nothing about internal access governance: it does not specify which Commission services may

query logs, on what legal basis, or subject to what authorisation.. Without clear internal access governance, the log architecture risks functioning as a de facto behavioural monitoring system rather than a narrowly scoped accountability mechanism.

2.4 QTSP Gatekeeping, Open Source, and the Security Gap

Channelling all Registry access through qualified trust service providers places compliance costs on SMEs and smaller actors, with no fee regulation, minimum service obligations, or alternative access pathway provided in the draft. Article 3 describes the Registry's components without imposing any open-licensing or independent-audit requirement, despite the Interoperable Europe Act's (Regulation (EU) 2024/903) stated preference for free and open-source solutions in public sector digital infrastructure. Article 16 leaves technical audits discretionary, with no defined content, external auditor requirement, or disclosure obligation. Alignment with the Cloud Sovereignty Framework is deferred to a point when the relevant services become available, which provides no meaningful commitment. The Registry will hold identity and authentication data for all economic operators placing regulated products on the EU market; the security architecture should reflect that significance.

We call on the Commission to:

- Clarify the relationship between mandatory Registry verification and the voluntary-use principle in Regulation (EU) 2024/1183 (eIDAS 2), including published guidance on how SMEs and non-EU operators can satisfy verification requirements without full EUDI Wallet compliance.
- Introduce mandatory notification and a grace period before verified status lapses, providing at minimum 60 days' notice and a 30-day renewal grace period, with interim continued registration pending renewal.
- Insert explicit log-access controls: specify which Commission services may access logs, on what legal basis and internal authorisation, and require annual transparency reporting on log access.
- Require that the Registry's core software components and the semantic repository be released under open licences consistent with the Interoperable Europe Act, and subject to independent code audit.
- Require full API documentation to be published under open, reusable licences to enable independent implementation of compliant DPP systems without proprietary dependency.
- Require independent security auditing, potentially involving ENISA expertise or oversight standards, with a summary published annually.
- Publish a proportionality assessment of the QTSP verification cost burden for SMEs and circular economy actors, and require that Registry access not be contingent on services that are unavailable or unaffordable to smaller participants.

3. Transparency, Public Access, and Civic Accountability

The Registry will contain information about products placed on the EU market and will be funded and managed by the Commission as a public institution. Yet the draft is framed almost exclusively around operator access and national authority oversight. The question of what citizens, civil society, and researchers can access, and on what terms, is largely absent from the text. This is inconsistent with the transparency rationale of ESPR itself, which premises the DPP system on easy access to product sustainability information for consumers and the market.

3.1 Public Access to Registry Data

The draft establishes a Registry with a secure public user interface under Article 3(a), but public in this context means accessible after verification. There is no provision for unauthenticated public search of registered DPPs, product categories, or operator registrations. Recitals of Regulation (EU) 2024/1781 explicitly frame DPPs as a tool to give easy access to product sustainability information. A Registry that is accessible only to verified economic operators and national authorities does not serve that purpose. While consumer-facing Digital Product Passport information may be accessed through product interfaces and delegated-act mechanisms under ESPR, the Registry itself remains a critical governance and verification layer for market oversight, traceability, and accountability. Limited public access to basic registration metadata would therefore serve an independent transparency function without compromising the security architecture of the system. A publicly accessible, unauthenticated read-only interface enabling civil society, journalists, and researchers to query basic registration information would not compromise security and would give effect to the parent Regulation's transparency objectives.

3.2 Semantic Repository Governance

Articles 12(6) and 12(7) provide that the semantic repository will be accessible via publicly documented APIs, free of charge. This is a positive provision and should be acknowledged. However, Article 11 gives the Commission exclusive control over data model versioning, and the draft contains no governance provisions for how stakeholder input, including from civil society and affected industries, is incorporated into semantic decisions. The Interoperable Europe Act (Regulation (EU) 2024/903) requires public sector interoperability efforts to involve stakeholder consultation. The semantic repository is a form of public digital infrastructure whose design will determine what counts as a valid DPP across all product groups for years to come. It should be governed accordingly, with transparent, participatory versioning processes rather than unilateral Commission discretion.

3.3 National Administrator Model and Democratic Accountability

Article 7 requires each Member State to designate a single national administrator as the gatekeeper for all national authority access to the Registry. This concentrates significant access-control authority in a single national body. The draft provides no requirements for transparency around how national administrators exercise this role: no reporting obligations, no public disclosure of which authorities have been granted access, and no accountability to national parliaments or data protection supervisory authorities. Decisions about which

authorities can access a Registry holding personal data about all economic operators in the country warrant democratic oversight, not merely internal administrative management.

We call on the Commission to:

- Require the Commission to establish a publicly accessible, unauthenticated read-only interface for basic Registry queries, including product category, operator status, and registration date, to give effect to the transparency rationale of ESPR without compromising security.
- Subject the semantic repository's governance to a formal stakeholder consultation process consistent with the Interoperable Europe Act; data model versioning decisions must not be exclusively within Commission discretion.
- Require national administrators to publish annual transparency reports disclosing the number of national authorities granted Registry access, the categories of access rights granted, and any access revocations.
- Extend the scope of Commission guidance under Article 15(1) to include public-facing materials accessible to civil society and consumers in all EU official languages.

---

4. Registry Availability, Incident Response, and Market Access Rights

The draft gives the Commission broad powers to suspend Registry access, impose measures against fraudulent use, and manage outages, without providing adequate procedural protections for operators whose market access depends on Registry functionality. Where the Registry is mandatory infrastructure for legal compliance, Commission-side failures and Commission-side enforcement actions must carry commensurate legal safeguards.

4.1 Suspension Without Notice and Market Access Consequences

Article 15(3) permits the Commission to suspend Registry access without prior notice in the event of malfunction, cyber-attack, or urgent security need. The draft provides no mechanism for operators whose compliance obligations are affected by an unplanned suspension: no force majeure provision, no temporary relief from registration requirements, and no explicit commitment that enforcement action will not be taken against operators for non-compliance caused by Registry unavailability. An operator unable to register a DPP because the Registry is down through no fault of their own faces potential market access consequences for a Commission-side failure. This is inconsistent with basic principles of proportionality and legal certainty.

4.2 Outage Records and Proactive Disclosure

Article 15(4) requires the Commission to record the duration and timing of Registry unavailability and make this information available upon request for at least five years. Disclosure on request is an inadequate accountability mechanism for a system on which

market access depends. Operators subject to market surveillance or customs controls during a period of Registry unavailability need to demonstrate that the failure was on the Commission's side. Proactive publication of outage records on a public website, updated promptly following service restoration, would significantly reduce the evidentiary burden on operators and would be consistent with ESPR's transparency objectives. The current on-request model shifts accountability in the wrong direction.

4.3 Fraudulent Use Provisions and Procedural Fairness

Article 17 empowers the Commission to take unspecified necessary measures where it identifies inappropriate or fraudulent activity, including activity linked to massive data download. The provision omits any definition of inappropriate use, any procedural requirement to notify the affected user before measures are taken, any right of appeal or review, and any proportionality requirement. Given that the Registry is mandatory infrastructure for market access, measures under Article 17 could suspend an operator's ability to place products on the market without any of the procedural safeguards that would accompany a formal enforcement decision under EU law. This is incompatible with the principles of legal certainty, proportionality, and the right to an effective remedy under Article 47 of the Charter.

4.4 Helpdesk Scope and Service Standards

Article 13 establishes a Commission helpdesk available during working hours for technical support. The provision carries no service level obligations: no response time commitments, no escalation procedures, and no remedies for helpdesk failures. For operators in non-Brussels time zones or with urgent compliance needs arising outside Commission working hours, this gap is material. The helpdesk also extends only to economic operators, value chain actors, and authorities; civil society and researchers have no equivalent access point for queries about the Registry or its governance.

We call on the Commission to:

- Insert a regulatory relief provision disapplying registration obligations during confirmed Commission-side Registry unavailability, with a mechanism for operators to obtain written confirmation of outage periods for use in enforcement proceedings.
- Mandate proactive publication of Registry outage records on a publicly accessible Commission website, updated within 24 hours of service restoration.
- Amend Article 17 to include a definition of inappropriate use; a requirement to notify the affected user before measures are taken except where immediate action is necessary to prevent harm; a right to submit observations; and a formal review mechanism consistent with Charter Article 47.
- Establish minimum helpdesk service standards including maximum response time commitments, an escalation procedure, and provision for urgent compliance matters arising outside standard Commission working hours.

Conclusion

The European Pirate Party supports the aim of the Digital Product Passport system and its role in advancing sustainability and circular economy objectives under ESPR. The Registry can support those objectives without creating a disproportionate identity and monitoring infrastructure. However, achieving that balance requires stronger safeguards than those currently provided in the draft Implementing Regulation.

More broadly, the draft continues a wider trend visible in the EU Digital Identity Wallet and QEAA framework debates: the gradual expansion of mandatory identity-linked digital infrastructures into ordinary commercial and administrative activities without corresponding rights protections. There is a real risk that centralised verification architectures become normalised without proportionality limits, decentralisation guarantees, or enforceable rights. Parliament and the Commission should resist that trend here.

We call on the Commission to revise the draft Implementing Regulation to:

- Conduct a formal data minimisation assessment with EDPS involvement before the Registry goes live, justifying each personal data category in Article 18 as strictly necessary;
- Insert operative provisions on data subject rights directly into the Regulation, with accessible procedures, timelines, and contact points;
- Require joint-controller agreements where Registry data is shared with national authorities for enforcement purposes;
- Establish a transparent equivalence mechanism for third-country trust service frameworks and alternative verification pathways;
- Introduce mandatory notification and grace periods before verified status lapses, with an appeal mechanism;
- Insert explicit log-access controls specifying who may access logs and on what legal basis, with annual transparency reporting;
- Require open licensing and independent audit of the Registry's software components, APIs, and semantic repository;
- Establish a publicly accessible read-only interface for basic Registry queries, consistent with ESPR's transparency rationale;
- Subject semantic repository governance to a formal stakeholder consultation process consistent with the Interoperable Europe Act;
- Require proactive publication of outage records and insert regulatory relief for operators affected by Commission-side unavailability;
- Amend Article 17 to ensure procedural fairness, proportionality, and Charter-compliant review rights before any market-access measures are imposed.

References

Charter of Fundamental Rights of the European Union (2012/C 326/02). Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf

Commission Implementing Regulation (EU) laying down implementation arrangements for the digital product passport registry (Draft). Ref. Ares(2026)4424976.

Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Retrieved from https://gdpr-info.eu/

Regulation (EU) 2018/1725 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies. Retrieved from https://eur-lex.europa.eu/eli/reg/2018/1725/oj

Regulation (EU) 2024/903 of the European Parliament and of the Council laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/903/oj

Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS). Retrieved from http://data.europa.eu/eli/reg/2014/910/oj

Regulation (EU) 2024/1183 of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1183/oj

Regulation (EU) 2024/1781 of the European Parliament and of the Council establishing a framework for the setting of ecodesign requirements for sustainable products (ESPR). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1781/oj

European Commission. Cloud Sovereignty Framework. Retrieved from https://commission.europa.eu/document/09579818-64a6-4dd5-9577-446ab6219113_en"

European Pirate Party Manifesto. Retrieved from https://europeanpirates.eu/manifesto/

European Pirate Party (PPEU) | europeanpirates.eu | May 2026