Home Appliance Europe

Bld. Brand Whitlock 114 B-1200 Brussels
hello@applia-europe.eu | **www.applia-europe.eu**
APPLiA Home Appliance Europe AISBL
Transparency number: 04201463642-88
VAT BE 0460 033 584

Policy Paper
June 2026

Policy Paper on the Digital Product Passport

The home appliance industry welcomes the digitalisation of product information as a future proof, more flexible alternative to paper documentation and a sound basis for digital economy. However, this does not automatically justify a broad, mandatory Digital Product Passport (DPP) model as currently envisaged by the European Commission. Such DPP requires a significant effort, while the home appliance sector, currently supporting 1 million jobs and contributing significantly to the EU GDP, is under high competitive pressure. It is therefore essential that the digital transition remains fair, pragmatic, and grounded in the "start small" principle, following a strict assessment of added value and necessity for each new obligation. It must also ensure legal certainty, protect trade secrets, and avoid imposing obligations before the relevant regulatory and technical parameters are clearly defined. For our industry this means leveraging the already existing and recognised systems such as the European Product Registry for Energy Labelling (EPREL) for products carrying an energy label and creating a harmonised framework that ensures that if a product is already legally required to carry a QR Code, no additional data carriers are added for overlapping requirements.

Key Messages:

- **Leverage existing infrastructures for the DPP,** such as EPREL, to avoid duplicating systems.
- **Start small, fair, and pragmatic** to avoid unnecessary complexity, reduce compliance burden, and safeguard competitiveness.
- **A Single EU QR Code for all legal information requirements**, ensuring simplicity, usability, and coherence across EU legislation.
- **Protect trade secrets and sensitive technical documentation** by ensuring that access is strictly limited, justified, and secured. Critical data must only be available on request.

- **Define DPP obligations only once the regulatory scope, governance model, access logic, and technical architecture are sufficiently specified.** Introduce any new obligations through a phased approach, including pilot phases and a realistic transition period

A Pragmatic Way Forward for the DPP

1. Avoiding Duplication and Build on What Works

The introduction of the DPP should follow a start-small, fair and pragmatic approach. In the context of home appliances, this requires building on existing, well-functioning systems rather than introducing parallel infrastructures. In particular, no new system should be created where an effective solution is already in place, in line with Article 9 of the ESPR (EU 2024/1781). Products already covered under the Energy Labelling Regulation, such as washing machines, refrigerators, and dishwashers, are required to provide detailed information to consumers and market authorities through EPREL. This information is also accessible via the QR Code displayed on the Energy Label attached to each product. **For this category of products, the DPP shall be provided in EPREL.**

EPREL hosts more than two million product registrations and it is equipped with robust verification and security mechanisms, ensuring the integrity and credibility of the data it contains. Establishing a separate DPP system for products already covered by EPREL would lead to unnecessary duplication, increased inefficiencies, and avoidable costs for both industry and public authorities.

At the same time, a meaningful rollout of the DPP requires sufficient regulatory specification before new quantitative obligations are imposed on companies. Without clarity on the exact data categories, access rights, governance obligations, and technical architecture, industry input on cost, feasibility, and timing will remain inherently uncertain. The same applies to the justification of each individual data point: before any obligation is imposed, it must be clearly demonstrated what concrete regulatory purpose the data serves, for whom it creates value, and why this value outweighs the associated burden. This risks undermining the quality of both consultations and impact assessments.

For this reason, any extension of DPP requirements beyond existing systems should follow a structured roadmap, including a pilot phase, clear technical and legal specifications, and realistic, predictable transition periods.

2. EPREL+ as a Single Data Entry Point for products with an Energy Label

In cases where DPP requirements extend beyond the current scope of EPREL, APPLiA proposes "EPREL+" as a potential approach. This concept builds on the existing EPREL system by evolving it to accommodate additional data requirements, rather than replacing it or creating a parallel structure.

EPREL+ would maintain EPREL as a single, trusted entry point while integrating new data fields only where there is a clear and justified need. It would also make use of web links to connect to manufacturers' websites or specialised databases, thereby ensuring flexibility and avoiding unnecessary duplication of data. This approach allows for a more efficient and scalable system architecture, while preserving coherence across different regulatory requirements.

Importantly, EPREL+ should ensure the identification of the legal representative established in the European Union and include functionalities that support market surveillance authorities in their enforcement activities, but without prejudice to established compliance assessment and verification procedures (cfr. section 6)

3. Protection of trade secrets and handling of technical documentation

The DPP framework must not result in the permanent online availability of complete technical documentation. Sensitive technical files, test reports and related compliance documents often contain trade secrets and cybersecurity-relevant information. Their inclusion in digital systems must therefore be limited to what is strictly necessary, subject to the highest cybersecurity standards, and based on a strict need-to-know and case-by-case access approach.

No general or blanket access to complete technical documentation should be granted, including for market surveillance purposes. Access to sensitive documentation should only be granted where justified in the context of a specific control or enforcement action. Given the growing cybersecurity risks affecting digital infrastructures, critical information should not be made accessible automatically, but should instead be made available bilaterally and only upon reasoned request

In addition, where authorities assess complex technical content, manufacturers should be consulted before conclusions are drawn, in order to avoid misinterpretation and disproportionate enforcement outcomes. The DPP should facilitate compliance and enforcement, but it should not become a central repository for broadly accessible confidential technical material.

4. Principles for DPP Data Requirements

Providing the data required under a Digital Product Passport entails significant costs and operational challenges for industry, which must be carefully considered when defining any new obligations. Data is often not readily available and must be generated, processed, and verified across complex and global supply chains, requiring substantial investments in IT systems and internal data management structures. Companies must adapt their classification systems, ensure data accuracy, and establish secure mechanisms for data storage and transfer, all of which generate both upfront and ongoing costs.

To ensure feasibility and effectiveness, DPP data requirements should follow these principles:

- **Demonstrated Added Value:** Only data with a clear, demonstrated added value for the relevant regulatory objective, user group, or enforcement purpose should be required. The mere possibility of future use should not justify mandatory data collection.
- **Verifiability**: All data must be measurable, enforceable, and auditable. Non-verifiable data risks undermining trust in the system.
- **Responsibility:** Economic operators should only be responsible for data within their control.This is particularly relevant in Original Equipment Manufacturer (OEM) and multi-tier supply chain constellations, where manufacturers may not have legal or practical control over all underlying technical data and documentation.
- **Proportionality:** The cost of generating and maintaining data must be proportionate to its value.
- **No Additional Burden for EPREL Products:** Products already covered by EPREL should not be required to provide additional data in the initial phase.
- **Product specific DPP:** The mentioned principles are very product group specific. A DPP for one product group should not automatically set any precedence for another. At the same time, limited horizontal minimum requirements may be appropriate where they facilitate interoperable data communication across product groups and supply chains.
- **Regulatory Clarity First:** Obligations should only be introduced once the applicable data scope, governance logic, access rights, and technical architecture are sufficiently specified. In the initial phase, requirements should be limited to the legal minimum and should avoid additional, non-essential deviations that would overburden supply chains.
- **Common Understanding:** Consultations and impact assessments should be based on clearly defined regulatory assumptions to ensure comparability of stakeholder input across sectors and authorities.

- **Phased Implementation:** Where requirements are novel or not yet operationally mature, implementation should start with pilot phases and realistic transition periods.
- **Confidentiality by Design:** Sensitive technical documentation, test reports, and other confidential compliance-related information should not be made permanently available online and should only be accessible where strictly necessary. Critical information must only be available on request

5. Principles for the DPP System

In times when the Union's economy is facing multi-lateral challenges, the EU strategy is to minimise effort and reduce the burden for all stakeholders. It is therefore critical to ensure that those who carry the investment for the system are also able to benefit from it. For the DPP system this means concretely:

➔ Learn from EPREL with respect to technology, functionalities and processes.
➔ Allow for those who have extensively invested in EPREL to start with these databases when introducing the DDP for their products.

Key learnings from EPREL and other databases that we suggest transferring to the DPP registry:

- Supplier/manufacturer verification with eSEAL (see also Art. 11 of the ESPR) or in future by means of the EU business wallet;
- Differentiated access management;
- Secured EU servers ensuring the necessary cyber security combined with asset minimisation on a need to know basis;
- Technical and operational details laid down in an Implementing Act (see also Art. 13(5) of the ESPR);
- Impartiality of the entity providing the service (European Commission);
- Weblinks possible (e.g. to existing databases, or existing supplier information);
- Possibility to allow for content data storage (see also Art 13(2) of the ESPR).
- Sensitive technical documentation should, as a rule, remain outside broad automated access repositories, regardless whether centralised or decentralised and be made available only under strictly controlled and justified conditions.
- The system architecture should support case-by-case disclosure of confidential information, including secure access controls, logging, and traceability of access to sensitive files.
- The framework should ensure interoperability between existing EU systems and sectoral solutions (e.g EPREL for products with Energy Labels) rather than replacing functioning infrastructures with a one-size-fits-all platform

6. Limitations of DPP for Market Surveillance

The DPP may play a supportive role in strengthening market surveillance, but it should not be misperceived as a help for market surveillance authorities per se. Its primary function is to provide access to relevant information, and where compliance-relevant information is concerned, the key challenge for authorities remains the verification of data in order to ensure fair competitiveness in the Single market. So while access to relevant product data for authorities could enable more effective cross-border enforcement within the Single Market the DPP **cannot serve as a tool to demonstrate or verify regulatory compliance. This must remain subject to established compliance assessment and market surveillance procedures.**

At the same time, it is important to recognise that the effectiveness of market surveillance ultimately depends on the resources, expertise, and enforcement capacity of Member States. Moreover, all market surveillance efforts will be in vain if the DPP cannot ensure the identification of a legal or natural person based in the EU and responsible for the compliance of the products concerned. For this reason, before any mandatory requirement on DPP data is introduced, **the DPP framework must ensure clear operator accountability, and impose the existence and identification of a legal representative established in the European Union**, being responsible for the compliance of the product in order to provide a reliable basis for enforcement actions.

As already mentioned, for security reasons the DPP should support market surveillance without turning into a repository of broadly accessible sensitive technical documentation. Enforcement access to confidential technical files must remain targeted, justified and secure. Where complex technical documentation is assessed, manufacturers should have the possibility to provide clarification in order to avoid incorrect technical interpretation.

7. A single EU QR code for the Single Market

Digital provision of product information has become a major undertaking under EU legislation. Increasingly, Union law permits or requires legally relevant information to be made accessible digitally via QR codes or comparable data carriers. While this transition can improve usability and reduce administrative burden, it also creates a growing risk of regulatory fragmentation. Without a horizontal approach, individual legal acts, including the ESPR, Energy Labelling, Batteries, Packaging and Critical Raw Materials requirements, may each mandate a unique QR code on the same product.

This would lead to a **stacking effect**, whereby a single product may be required to display multiple QR codes or support multiple parallel digital compliance pathways. Such fragmentation would create consumer confusion, reduce the effectiveness of digital

information, increase operational complexity for manufacturers, and undermine the Union's broader simplification agenda.

Even the Digital Product Passport (DPP), which is viewed as a way to unify information, carries this risk. Because the DPP is created under several different laws and implemented on a sector-by-sector basis, its "data carrier" risks becoming just another isolated QR code added to the product.

To avoid the 'stacking effect' of multiple regulatory markings, APPLiA advocates for a **Single EU QR Code** governed by a horizontal legal framework. This approach ensures that if a product is already legally required to carry a QR code, no additional carriers are added for overlapping requirements. Such a QR code would function as a harmonised entry point to access the potential DPP, among other EU legal requirements, to ensure coherence across overlapping legal requirements, while providing operator accountability by allowing for the mandatory identification and authentication of an economic operator being based in the EU. This would preserve prior investments, avoid duplicative compliance architectures and support a more efficient implementation of the future DPP.

To ensure a pragmatic and legally sound implementation, the framework for the single EU QR code should be based on the principles set out in the APPLiA "**Strategy Paper on the Single EU QR Code"**. This includes, in particular, clear mechanisms and rules for QR code generation, maintenance, updates, and redirection logic throughout the product lifecycle. A well-designed Single EU QR Code would provide a simple and intuitive consumer-facing entry point, contributing to simplification, legal certainty, stronger market surveillance and better usability across the Single Market.

Reference contact
Michał Zakrzewski *Senior Policy Director, Digital & Competitiveness*
michal.zakrzewski@applia-europe.eu

Reference contact
Iulia Florea *Junior Policy Officer, Digital & Competitiveness*
iulia.florea@applia-europe.eu