REPORT 2026

Preparing for the Digital Product Passport

How to navigate the Digital Product Passport for SMEs in the circular economy today

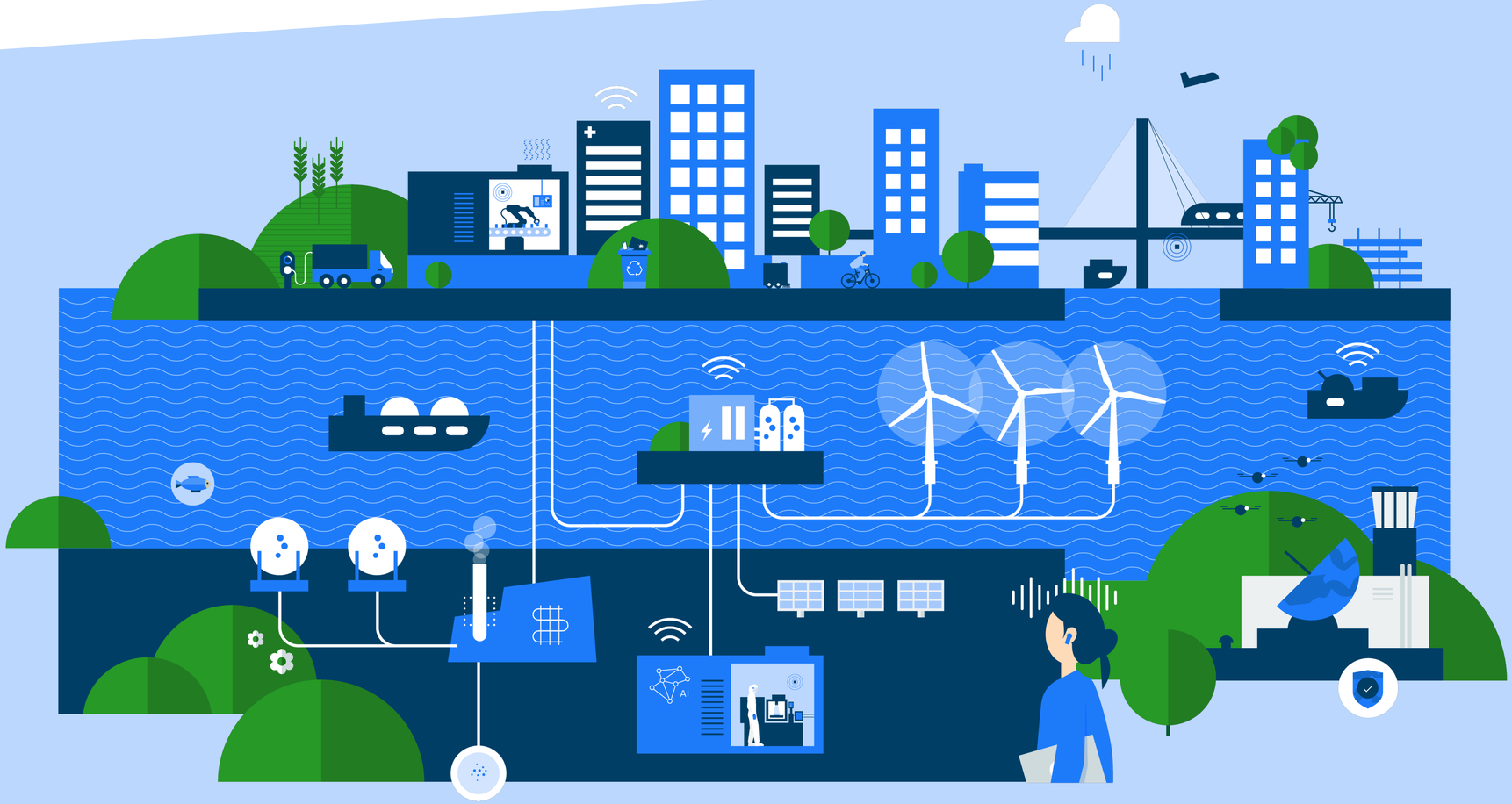


Table of contents

Are companies ready for the Digital Product Passport?

Small and medium sized enterprises (SMEs) across Europe are entering a new era of product transparency and sustainability. As part of the European Union's broader push toward a circular economy, companies will soon be required to share product information in a standardized digital format known as the Digital Product Passport (DPP). This report offers a practical introduction to the DPP concept, its regulatory foundations, and its implications for SMEs – particularly those preparing for upcoming requirements under the Ecodesign for Sustainable Products Regulation (ESPR).

The Digital Product Passport is more than a compliance tool. It is a digital dataset that travels with a product throughout its lifecycle, containing structured information about materials, carbon footprint, repairability, and end-of-life options. Via technologies like QR codes or RFID tags, the DPP can enable better decision making across value chains, support circular business models, and strengthen customer trust through transparency.

While the DPP will eventually apply to many product groups, this report places special emphasis on the on the sectors that are first in line for DPP. For instance, companies from the production industry, whether involved in design, manufacturing, distribution, or repair, will need to adapt their data systems, supplier relationships, and product documentation to meet new expectations.

The Digital Battery Passport, already mandated under the EU Battery Regulation, provides a concrete example of how the DPP might affect the value chain.

This report supports Danish small and medium sized manufacturing companies in preparing for compliance with the DPP. While key technical requirements – such as specific data protocols and data points – have not yet been defined due to the pending delegated acts, the regulatory direction is clear: companies will be required to establish structured, accessible, and reliable product data systems.

Rather than waiting for full regulatory clarification, companies can already begin preparing. This report outlines the origin and regulatory foundation of the DPP and analyzes how industry actors are currently approaching its implementation. A central premise is that understanding what is already known enables companies to make informed strategic decisions and allocate resources proactively.

Accordingly, the report focuses on the elements that are presently clarified, including available data carrier options and the considerations underlying their selection. For instance, establishing robust internal data structures will significantly ease future compliance once the delegated acts are adopted. Further work on data quality will be developed in 2026 as part of FORCE Technology's continued efforts in this field.

In addition, companies that already share product or supply chain data should consider cybersecurity readiness as a related and immediate priority. The mechanisms required to ensure secure data exchange today closely resemble those that will be necessary under the DPP. Strengthening cybersecurity and access control frameworks at this stage will therefore not only mitigate current risks but also support future DPP compliance.

The report is guided by the following research question:
"How can Danish small and medium sized manufacturing companies prepare for the upcoming Digital Product Passport?"

Methods and limitations

This report is grounded in a qualitative research approach combining desk research with semi-structured interviews to explore perspectives and practices related to the preparation for the DPP. The methodology was designed to capture both existing knowledge and lived experiences from key stakeholders across the industry.

Desk research

The desk research phase involved a review of existing literature, policy documents, industry reports, and technical guidelines relevant to the topic. Sources included publicly available materials from EU regulatory bodies, sector specific white papers, and internal documentation. This phase helped establish a foundational understanding of the regulatory landscape, technological frameworks, and strategic priorities shaping the development and implementation of DPPs.

Semi-structured Interviews

To complement the desk research, semi-structured interviews were conducted with a diverse group of actors from Danish industry. The interviews were designed to elicit nuanced insights into practical challenges, opportunities, and organizational responses to DPP-related initiatives. Interviewees were selected based on their direct involvement in relevant projects or decision making processes, ensuring the relevance and depth of the data collected.

The semi-structured format allowed for flexibility in exploring emerging themes while maintaining consistency across core topics. Interviews typically lasted between 30 and 60 minutes and were conducted either in person or via video conferencing. Notes and transcripts were analyzed thematically, with attention to recurring patterns, contradictions, and sector specific concerns.

Limitations

While the combination of desk research and interviews provides a robust basis for analysis, the findings are inherently shaped by the perspectives of the selected participants and the availability of public documentation.

Ecodesign – where it all began

What is today the framework for the Digital Product Passport (DPP) has its roots in the EU's Ecodesign Directive (2009/125/EC). The original goal was simple and concrete: to reduce energy consumption and the environmental impact of energy related products. A tangible example, familiar to many from everyday life, is the labeling of washing machines – the old A+/A/B/C labels made it possible for consumers to choose models that use less electricity, which contributed to a real decrease in energy consumption across the EU, while also saving consumers money on their electricity bills.

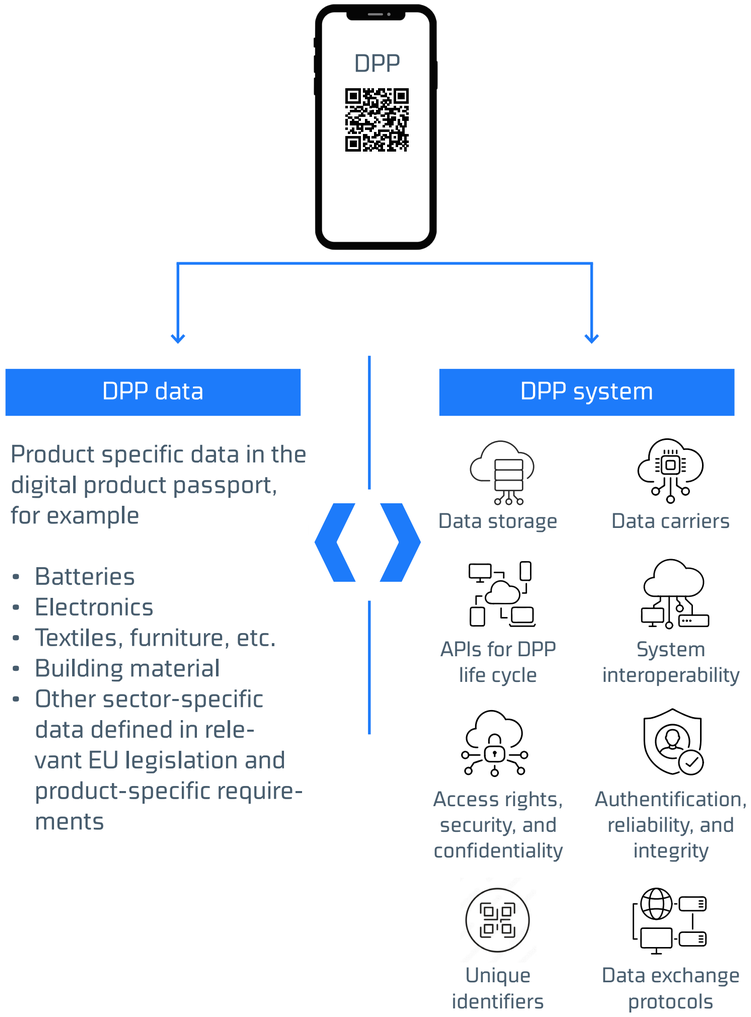
From energy efficiency to circularity - ESPR

The success of the Ecodesign Directive set the stage for a broader shift in ambition within the European Green Deal. The Ecodesign for Sustainable Products Regulation (ESPR) (EU) 2024/1781 is the upgraded framework – where the 2009 directive focused on energy, ESPR aims for a much broader sustainability goal, namely circularity, durability, reparability, and recyclability. ESPR also marks the transition from a directive to a regulation: Whereas directives previously had to be transposed into national law, a regulation applies directly in all member states. As a result, the requirements become more uniform across the EU and directly applicable to businesses operating within the internal market.

So, ESPR is therefore not just about reducing energy consumption; it must also ensure that products are designed in an environmentally friendly way, so that products, materials, etc., can be kept in circulation and resources are not lost in subsequent stages.

What about the Digital Product Passport?

A central tool in the ESPR initiative is the DPP. One way to describe the DPP is an enhanced version of a traditional table of content. It will be a structured register that collects information about material composition, repair options, recycling instructions, the origin of critical materials, and other metadata needed by manufacturers, repairers, recyclers, regulatory authorities, and consumers in a circular economy. When this information is machine readable and linked to a unique identifier and a data carrier (such as a QR code or RFID), the data becomes both practically usable and reusable, enabling services and business models based on product data. On the right side, we have listed some of the horizontal requirements that the DPP must include



Source: Dansk Standard DS-hæfte 67:2026

Who is targeted?
It is, of course, crucial to determine who this legislation targets. Are you subject to it? Under theESPR, the obligations apply to so-called “economic operators.” According to the regulation, economic operators include manufacturers, authorized representatives, importers, distributors, dealers, and fulfilment service providers.

In practice, this means that the economic operator placing a product on the EU market, most often the manufacturer, bears the primary responsibility for creating and maintaining the DPP. Other actors may step in where their role in the supply chain requires it. Companies may also choose to rely on third-party service providers to collect, manage, or store DPP data, but the legal responsibility remains with the economic operator that places the product on the EU market.

The ESPR also refers to “independent operators,” as actors outside the manufacturer’s organization working with products during their lifecycle. This includes companies involved in activities such as repair, refurbishment, remanufacturing, maintenance, and waste management. As a result, repairers, refurbishers, recycling companies, suppliers of repair equipment, and publishers of technical repair instructions may need access to certain product information through the DPP. This can include repair manuals, spare parts lists, and material composition data, which enable independent operators to repair, reuse, refurbish, or recycle products more effectively. When it comes to remanufacturing, the ESPR establishes a clear principle: the economic operator that places a product on the market or markets it under its own name assumes the same obligations that would normally apply to the manufacturer. This means that if a company significantly modifies a product and reintroduces it to the market under its own name, it will generally be required to fulfil the same responsibilities as a manufacturer. This includes the obligation to provide a DPP where the product is covered by a delegated act under the ESPR.

The precise rules for DPPs, including which products are covered, what information must be included, and whether the passport applies at model, batch, or individual product level, will be defined in upcoming product-specific delegated acts adopted under the ESPR.

The first Digital Product Passport implementation
The Digital Battery Passport (DBP) is the first fully established product passport in the EU, embedded directly in the new Battery Regulation (EU) 2023/1542, which in Article 77 requires an electronic register for relevant battery types. The DBP becomes mandatory for certain batteries, including large batteries for electric vehicles and industrial applications, with effective dates set in the regulation.

The DBP serves as a concrete pilot, both technically and organizationally. It demonstrates how data should be structured, which actors must provide information, and which workflows need to be in place throughout the supply chain, long before other sectors face similar requirements. Several industry projects and market examples, for instance car manufacturers already issuing battery passports for their models, illustrate how solutions can look in practice.

At the same time, we see signs of a natural evolution from this specific battery solution towards broader, more flexible requirements within the ESPR framework. While the Battery Regulation explicitly points to QR codes as a practical data access channel, ESPR and related technology discussions open up for a DPP to also be linked to other data carriers, such as RFID tags or other machine readable identifiers, to enable faster scanning and industrial automation. It is therefore plausible that, over time, both technological improvements and harmonization between the battery rules and ESPR’s more general requirements will happen.

In other words, the battery passport is the EU’s practical pilot project for DPPs: it tests the technology, clarifies responsibilities and processes, and at the same time sends clear signals about how the future DPP ecosystem may function at scale.

Framework of legislation and delegated acts
It is important to understand that ESPR is a framework legislation. This means that the overall goals and principles are set out in the regulation itself, while the precise sector- and product specific requirements – including what a the DPP must contain for textiles, construction, or electronics – will only be determined in subsequent delegated acts. Horizontal requirements information across

sectors, will therefore be relatively uniform, with many already established, while the detailed requirements will be rolled out sector by sector according to a planned timeline. Thus, companies should start now to structure their data and IT setup to be ready for the introduction of the sector specific requirements.

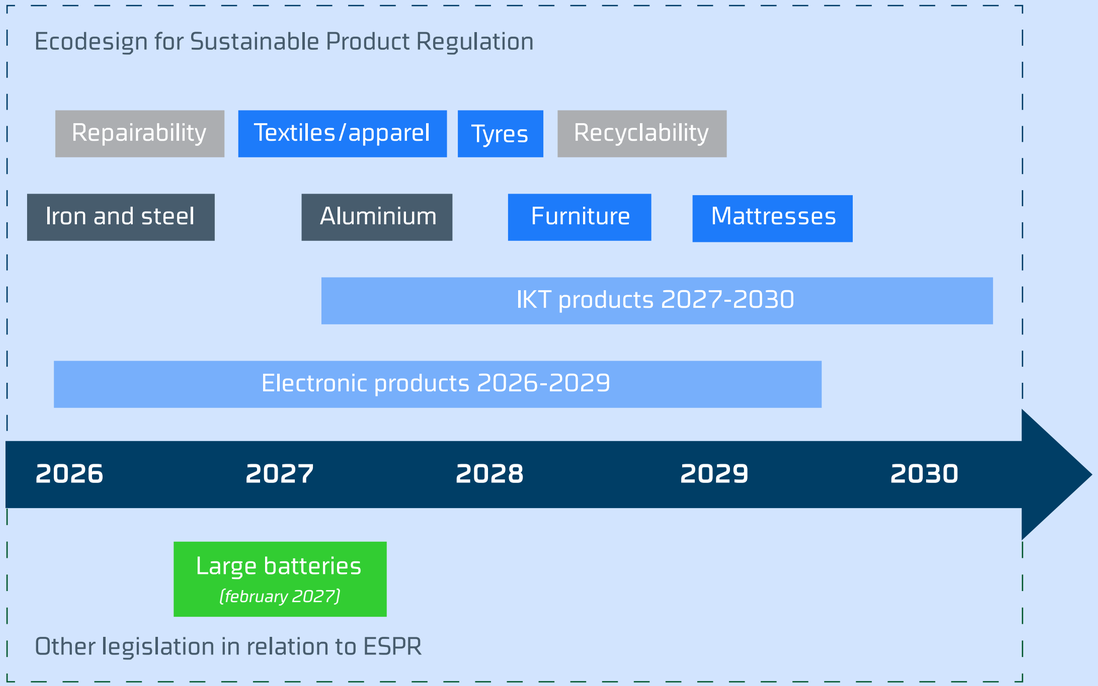
For companies, this development brings both obligations and opportunities. Yes, there will be new requirements for documentation and data management. But at the same time, DPPs open the door to increased reuse value, new services, and better relationships with customers, authorities, and partners. Starting to structure your product data now is therefore not just compliance preparation – it is an investment in the business model of the future.

While the regulatory framework outlines clear objectives and structural requirements, there is a significant distinction between legislative intent and practical implementation. A regulation of this magnitude, affecting all products placed on the European market, introduces substantial operational, technical, and organizational challenges. This complexity has been further amplified by the uncertainty associated with the Omnibus legislative developments, which have influenced expectations and planning assumptions across industry.

Below the timeline, we highlight other EU legislation related to ESPR. While ESPR establishes the framework for Digital Product Passports (DPP), several sector-specific initiatives introduce complementary requirements for product information and sustainability data. These include the Construction Products Regulation (EU) 2024/3110, the Packaging and Packaging Waste Regulation (EU) 2025/40, the proposed Toy Safety Regulation (COM(2023) 462), the proposed revision of the Detergents Regulation (COM(2023) 217), the Energy Labelling Regulation (EU) 2017/1369, and the Right to Repair Directive (EU) 2024/1799. Over time, the DPP is expected to serve as a common digital access point for product information across EU legislation.

As the following sections demonstrate, the experiences of the interviewed companies show that translating regulatory requirements into practice is far from straightforward.

Expected timeline for the ESPR working plan



Source: European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0187

Regulatory uncertainty and timing

Across industries, companies identify regulatory uncertainty as one of the most significant barriers to implementing the DPP. The lack of clarity on EU requirements and shifting timelines creates hesitation, making it difficult to justify investments or plan implementation strategies. Thus, unclear requirements and scope remain a major obstacle for companies preparing for DPPs. Grundfos highlights the challenge of moving forward without knowing the full data requirements. The company stresses that without clear specifications, it is impossible to determine which systems to upgrade or whether new tools are needed. This uncertainty prevents building a solid business case and securing funding for IT investments. Grundfos also points out that the scope of application, whether passports apply at product variant, family, or batch level, remains unresolved, adding complexity to planning

Short term planning and risk avoidance characterize how many companies respond to uncertainty around DPPs. Some companies adopt a cautious approach due to unclear relevance and timing. Nordic Firefly admits that their perspective is limited to short term horizons, often planning only six months ahead. They acknowledge uncertainty about how DPP will affect their products and processes, which discourages long term commitments [2]. Similarly, Nordsense explains that compliance decisions are guided by perceived difficulty and economic impact. If the consequences are unclear or minor, the topic does not receive significant attention [3].

Need for predictability and trust is central to companies' ability to plan for DPPs. Textile stakeholders emphasize predictability as a critical requirement. Markus Hatting from Textile Revolution argues that companies need a clear roadmap with milestones over the next decade to plan effectively. He warns that repeated delays and changes, such as those seen with Omnibus and CSRD, have undermined trust in the regulatory process. Without consistent progress, businesses hesitate to invest, fearing that requirements will shift again [6].

For smaller firms, uncertainty is particularly problematic. The company Our Units explains that legislation could serve as a catalyst for action, enabling her to convince management to allocate resources. However, with many legislative initiatives still postponed or unclear, it is difficult to make a compelling case internally. The company notes that the secondary legislation will make planning far easier [7]. Thus, currently it is clear that the companies need to know which data points will be required before they can begin preparations. Without this clarity, starting work is considered pointless. More detailed requirements could provide competitive advantages for some firms, but they also increase complexity and cost [8].

From projects in FORCE Technology, we know that some companies are already taking proactive steps by mapping their entire value chain in detail to prepare for upcoming requirements. They view this effort as a strategic investment, expecting it to become a competitive advantage once stricter rules are enforced. For these firms, tougher regulations would level the playing field, shifting competition away from price alone. They also anticipate that increased transparency will highlight their commitment to responsibility and sustainability, which are attributes they hope consumers will reward by choosing more sustainable products.

"At least Grundfos is a bit reluctant to jump ahead without knowing full data requirements. (...) we think it could be a waste of time and money to start something up without really knowing concrete requirements."

Grundfos

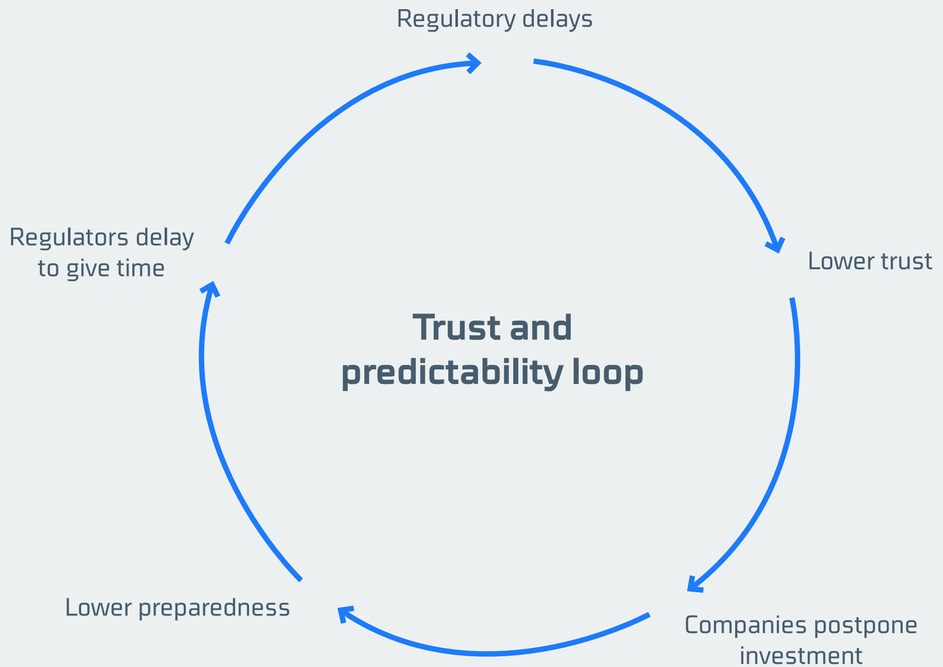
"I have to admit that our perspective is not very long right now. We are looking maybe six months ahead at a time. That's about what the strategy can handle."

Nordsense

Sector specific considerations add another layer of uncertainty to DPP implementation, as companies struggle to anticipate when and how their products will be affected. One standardization and product regulation expert points out that implementation begins with specific product categories, such as large batteries, before expanding to others. This phased approach could help manage complexity but also adds uncertainty for sectors unsure when their products will be included [4]. Discussions with GS1 confirm that even basic governance questions, such as how updates after repairs will be handled, remain unresolved [5].

”We have a real wish to do this. It’s not just to satisfy someone we want to make sure the products we make are as good as they can be with what we can get. But it’s really annoying that we can’t get clarity. We simply can’t get parts from anywhere else than China right now. We’ve tried research projects, but it takes too long be-fore we have an alternative, and it becomes way too expensive.”

Nordic Firefly



Source: FORCE Technology

Data management and system integration

Data management emerges as one of the most critical challenges in preparing for DPPs. Across sectors, companies emphasize that readiness is not simply about collecting information but ensuring its accuracy, structure, and accessibility. Poor quality data undermines the entire purpose of DPP, making validation and governance essential steps before integration.

Data readiness and internal consolidation are key steps for companies preparing for DPPs. Several firms acknowledge that their first priority is to assess what data they already have and to identify gaps. Grundfos illustrates this phased approach: starting with mapping existing data points, prioritizing them, and then addressing missing elements such as circularity metrics. This process requires significant internal effort before any external platform can be adopted. Without this groundwork, even advanced tools cannot deliver value [1]. Similarly, companies in textiles stress that data must be correct and processes understood; digitization without process clarity leads to failure [4].

System limitations and the need for new tools are evident as current enterprise platforms cannot fully support DPP requirements. Existing ERP and PLM systems often fall short of supporting DPP requirements. While these systems manage core product data, they rarely accommodate lifecycle calculations, circularity indicators, or dynamic content distribution. Grundfos notes that machine readable formats cannot rely on static PDFs, prompting investment in content delivery platforms and potentially new lifecycle assessment tools [1]. Smaller firms echo this concern, pointing out that resource constraints make in house development unrealistic, increasing reliance on third party solutions [7].

Verification and governance are non-negotiable for ensuring the integrity and trustworthiness of data in DPPs. Textile stakeholders argue that without verification, DPP risks becoming "cowboyland," where unvalidated claims erode trust [6][7][8]. To ensure valid data companies explore workflows that enforce validation before data entry, ensuring traceability and accountability. To strengthen compliance, organizations could implement governance processes that require users to document data sources and complete validation checks before uploading information, ensuring only accurate and reliable data enters the system.

Standardization to reduce complexity is essential for scaling DPP implementation and avoiding redundant work across multiple platforms. The absence of standardized formats creates inefficiencies, particularly for suppliers serving multiple customers. One expert points out that in the current situation divergent protocols force companies to re-enter identical data across several portals, wasting time and increasing error risk. Thus, it is important that the DPP does not add to processes like this. Harmonized standards would allow interoperability and scalability, enabling firms to prepare once and distribute broadly [4]. GS1 discussions confirm that alignment on identifiers and classification systems, will be vital for consistent data exchange [5].

Traceability and unique identifiers present significant challenges for companies as they prepare for DPPs. Beyond data quality, firms anticipate difficulties in assigning and managing unique identifiers for products and components. This complexity grows when passports must reflect updates after repairs or refurbishment.

"If the requirement for the DPP is that it has to be machine readable, then the PDF is not enough. We already know what kind of tools we need – we need some content delivery platforms to be able to have dynamic content distribution."

Grundfos

"When you digitalize your data... you also need to know your processes. Because otherwise you run all sorts of risks that your digitalization will not work."

Standardisation and Product Legislation Specialist

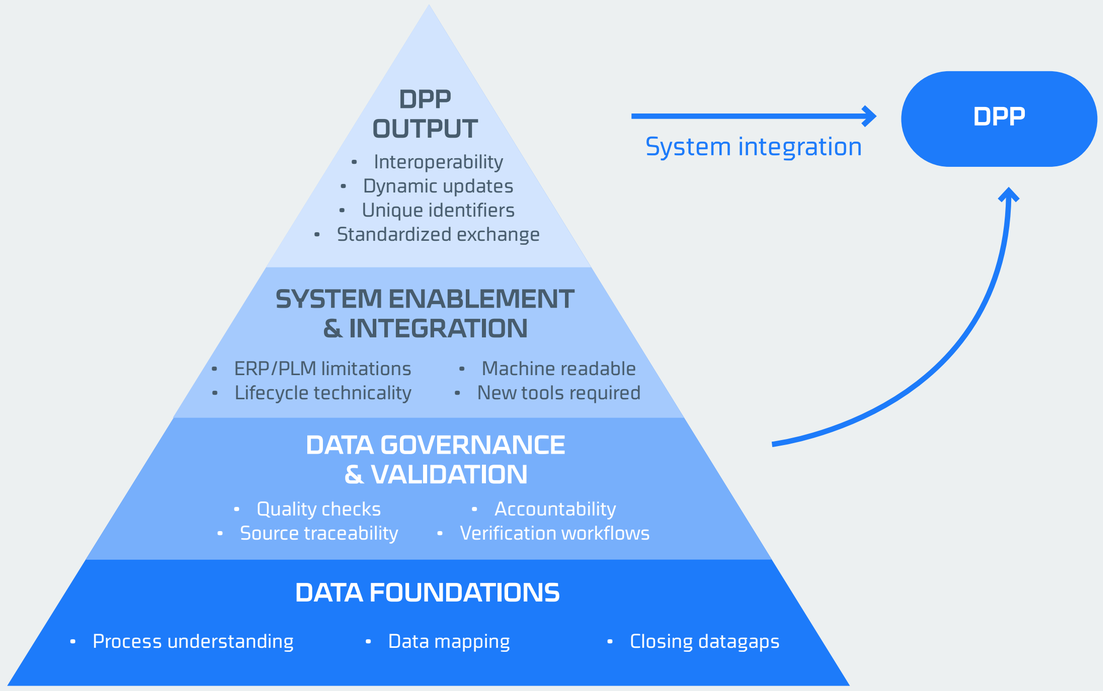
While some companies already serialize items at batch level, moving to item-level identification could require significant changes in labeling and IT infrastructure [9].

In summary, companies agree that successful DPP implementation hinges on three pillars: robust internal data governance, investment in systems capable of handling new requirements, and adoption of standardized, verifiable formats, which may impose great challenges for many companies. Furthermore, practical experience from company visits reinforces these challenges. Many SMEs face the reality of moving from almost no digital infrastructure to full scale data management in a very short time. Upcoming requirements demand complete control over both static ("dead") data and dynamic ("live") data, yet this is often where companies struggle the most. For firms with limited experience in digitalization or systematic process management, the transition becomes significantly harder. Helping companies establish basic data structures and digitize information has proven essential, as these foundational steps enable them to meet compliance requirements and avoid falling behind when DPP obligations take effect

"I am very positive about this happening. I actually believe it can solve a lot of problems, but it is essential that emphasis is placed on ensuring the data is correct. Yes. And that there is also focus on helping medium-sized manufacturers to get correct data"

Standardisation and Product Legislation Specialist

The DPP data readiness pyramid



Source: FORCE Technology

Transparancy vs. competitive risks

Transparency is widely recognized as a cornerstone for trust, compliance, and advancing sustainability goals within the DPP framework. On one hand, detailed disclosure can create strategic advantages for companies that are well prepared. One company argues that greater granularity in data could strengthen competitive positioning for firms with robust processes, even if it adds complexity internally. For others, however, the same level of detail may impose disproportionate burdens, particularly on smaller players, and expose sensitive business practices [8]. This asymmetry underscores why transparency is not universally perceived as neutral, it can reshape market dynamics and intensify competition.

Concerns also extend to supply chain relationships. A standardisation and product legislation specialist points out that current legislation does not grant manufacturers the right to demand accurate data from sub-suppliers, leaving producers accountable for compliance without reciprocal leverage [4]. This imbalance heightens the risk of incomplete or unreliable disclosures while amplifying pressure on primary manufacturers to validate upstream information.

Several companies advocate for controlled transparency, where data shared externally is subject to rigorous validation processes. One example to reach this is to implement an internal governance structure to ensure that only verified information enters the passport system, reducing the likelihood of errors and safeguarding trust. This approach reflects a broader industry consensus that transparency must be coupled with accountability to avoid reputational and operational risks.

In sum, while transparency is essential for achieving the objectives of DPP, its implementation must navigate a delicate equilibrium between fostering trust and protecting strategic interests. Companies agree that success will depend on harmonized standards, robust validation mechanisms, and governance models that enable openness without exposing firms to undue competitive risk.

”It’s data they need to go out and get from their suppliers, and sometimes even further down, not just tier one, but maybe tier two or tier three, they need to collect the information. [...] And in the end, it’s me as the manufacturer who puts products on the market that is responsible. And if you look at the EU’s digital product passport as it stands now, it starts with the manufacturer. Yes. It does not start with the subcontractor.”

Standardisation and Product Legislation Specialist

“What happens when you start setting all these detailed requirements... it becomes very hard for small companies. [...] There are so many things for a small company to overcome besides the usual administration, which doesn’t add anything to the business. And if you’re not in, then you’re out.”

Nordic Firefly

References
[1] ID Identity
[2] Textile Revolution
[3] GS1 Denmark
[4] Standardisation and Product Legislation specialist
[5] Nordsense
[6] Our Units
[7] Grundfos
[8] Nordic Firefly
[9] United Textile Group

Why to get started and how?

The DPP can enable new service offerings, support repair and resale models, strengthen brand transparency, and provide deeper insight into product lifecycle performance. At the same time, it can improve customer communication, support ESG documentation, and reduce compliance risk as sector specific requirements are introduced. Starting early allows companies to take a strategic approach, gradually align systems and suppliers, and avoid rushed implementation once delegated acts take effect. In this context, FORCE Technology supports companies in navigating the regulatory framework and translating DPP requirements into practical, future proof solutions that align with their overall business strategy.

As companies begin navigating the emerging DPP landscape, it is already possible to take meaningful steps that move the organization from theory to practical implementation. Even though much of the regulatory framework is still evolving, businesses can strengthen their understanding of current data practices, explore relevant technological enablers such as data carriers, and consider the cybersecurity implications of future digital transparency requirements. These early efforts create a solid foundation for the guidance presented in the following chapters, where the focus shifts from conceptual foundations and data collection to concrete technologies, security considerations, and five actionable steps companies can take to get started.

The following examples are illustrative and intended to inspire potential business development opportunities. Actual implementation must align with applicable regulatory requirements, including accessibility, interoperability, and data protection rules.

Turn every product into a revenue channel
A manufacturer uses the DPP as a digital gateway to guide customers toward certified spare parts, service subscriptions, and upgrades. While maintaining open access to required product information, the company strengthens its aftermarket presence and builds recurring revenue streams beyond the initial sale.

Design smarter, not just greener
By analyzing repair trends and lifecycle patterns linked to the DPP (in compliance with data protection regulations), a company identifies recurring component failures. This insight supports targeted redesign, reduces warranty costs, and improves product durability.

From product sales to lifecycle services
Using DPP to structure product configuration and maintenance data enables subscription-based services, predictive maintenance models, and performance guarantees. The company shifts from transactional sales to long-term lifecycle relationships.

Participate in the secondary market
By leveraging DPP to verify authenticity and document refurbishment, a company can actively engage in resale markets. This supports circularity while protecting brand reputation and maintaining visibility across multiple product lifecycles

Data carrier technologies for Digital Product Passport

DPPs require a reliable mechanism to link a physical product to its digital information across production, logistics, use, and end-of-life processes. Data carrier technologies provide this link by enabling identification, data access, and interaction at different points in the value chain. However, no single technology satisfies all DPP requirements equally. Factors such as latency, scalability, security, area coverage, cost, and ease of deployment vary significantly between solutions and directly influence their suitability for specific DPP use cases. The following sections compare key data carrier technologies based on these criteria and assess their relevance for DPP implementation.

RFID

RFID technology identifies items using electromagnetic fields. Its advantages include the ability to read multiple items simultaneously without a direct line of sight, high scalability, and well established standards.

Drawbacks include signal interference from materials like metals and liquids, and a higher cost compared to barcodes. While small scale pilots are straightforward, large scale deployment requires radio frequency planning and integration with backend systems.

Latency, Scalability, Security, Area Coverage: It offers very fast, millisecond level read speeds. Scalability is good with proper system architecture, though large deployments need careful planning. Security can be robust with AES encryption but relies on correct configuration. Coverage ranges from a few meters for passive tags to over a hundred meters for active ones.

DPP Suitability: Excellent for logistics; less so for direct consumer use unless combined with NFC.

Barcode

Barcodes are printed visual codes. Their main benefits are extremely low cost, universal recognition, and simple deployment. Limitations include the need for a direct line of sight, manual scanning, and vulnerability to copying. Implementation is one of the simplest among all technologies.

Latency, Scalability, Security, Area Coverage: Scanning is fast, but overall speed is limited by human operation. While cheap to produce in mass volume, scaling operations require more manual labor. No inherent security and require additional features like digital signatures for protection. Effective range is typically centimeters.

DPP Suitability: Serves as the best universal and cost effective baseline option.

NFC

NFC is a short range, high frequency form of RFID. It is highly consumer friendly as it works with smartphone taps and supports secure cryptographic elements. The primary constraint is that it has a very short operating range, and cost is higher than other possibilities. It i easy for consumer interaction, but secure enterprise integration is more complex.

Latency, Scalability, Security, Area Coverage: It enables near-instantaneous communication. It is designed for one-to-one interactions, not bulk reading. Security is a key strength, supporting features like tokenization, though it can be vulnerable to relay attacks. Range is limited to a few centimeters.

DPP Suitability: Excellent for direct consumer engagement and anti-counterfeiting applications.

BLE beacons

Bluetooth Low Energy (BLE) beacons broadcast signals for proximity detection and location. Advantages are low power consumption, compatibility with smartphones, and inexpensive hardware. Downsides include inaccurate distance measurement and a need for environmental calibration. Pilots are easy, but large scale deployment requires sophisticated algorithms.

Latency, Scalability, Security, Area Coverage: Response time ranges from 100 milliseconds to several seconds. Scalability is possible, but dense deployments can lead to signal congestion. The advertising signals are generally unauthenticated, requiring security measures like rotating identifiers. Coverage is typically up to 30 meters indoors.

DPP Suitability: Fits niche roles like reusable packaging or smart packaging.

Ultra-wideband

Ultra-Wideband (UWB) uses precise time-of-flight measurements for location. It provides centimeter level accuracy, is resistant to signal reflection, and has low latency. Major constraints are higher cost, the need for fixed infrastructure (anchors), and limited market adoption. Implementation is complex but feasible with developer kits.

Latency, Scalability, Security, Area Coverage: It delivers very fast location updates. Scalability is managed through anchor networks. It supports secure range protocols, making it highly resistant to spoofing. Each anchor covers tens of meters.

DPP Suitability: Reserved for niche applications involving high value asset tracking.

Infrared sensors

Infrared sensors detect presence, heat, or proximity. They are low cost, energy efficient, and provide immediate detection. Their weaknesses include requiring a clear line of sight and susceptibility to environmental interference. Simple motion sensors are easy to deploy, but thermal imaging requires calibration.

*Latency, Scalability, Security, Area Coverage:*They operate in near real time. Scaling a network of simple sensors is easy, but high resolution imaging is costly. They have a low RF attack profile but can raise privacy concerns. Coverage ranges from a few meters for motion sensors to room scale for cameras.

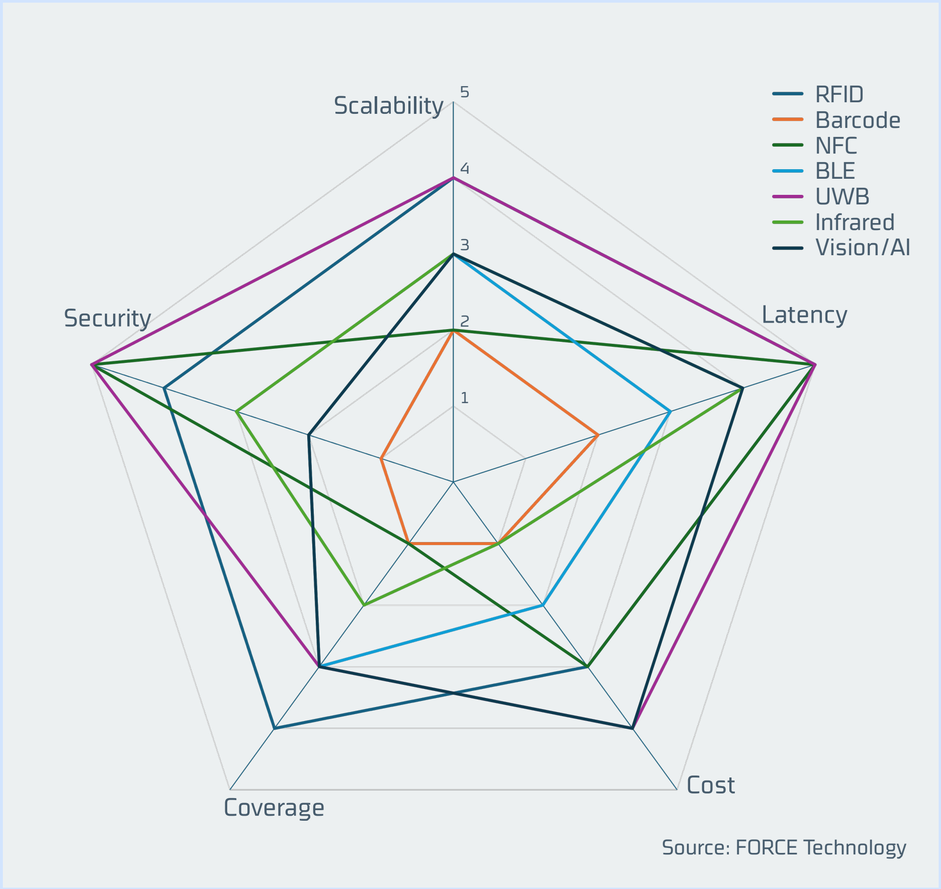
DPP Suitability: Not suitable as a primary data carrier for DPPs.

Vision/AI:

Computer vision and AI can capture rich, contextual data and is highly adaptable. Drawbacks include sensitivity to lighting conditions, high computational demands, and privacy risks. Prototyping is simple with pre-trained models, but production systems need custom training and infrastructure.

Latency, Scalability, Security, Area Coverage: ISpeed can be very fast with optimized computing. Scalability depends on network bandwidth and edge inference capabilities. It is vulnerable to adversarial attacks and privacy breaches. The coverage area is defined by the camera's field of view and resolution.

DPP Suitability: Highly effective for applications like automated recycling, sorting, and visual identification.



Source: FORCE Technology

Barriers related to cyber security

Confidential information within DPPs such as intellectual property details, trade secrets, regulatory and compliance data makes them attractive targets for cyberattacks for malicious actors in current geo-political scenarios. Thus, it is very important to understand the need to secure DPP data and its underlying system that stores, processes, transmits and communicates DPP data. As it is vital to maintain trust, operational resilience, and adherence to regulations like GDPR, Cyber Resilience Act (CRA) and NIS2.

The role and importance of DPPs
DPPs contain vital information for verifying supply chain authenticity, compliance and environmental impact data. A DPP is an apparatus for stakeholders to track material sources, confirm green credentials, and access disposal guidelines. DPPs also enhance consumer confidence and help product manufacturers meet regulatory demands, while also being pivotal in monitoring carbon emissions and enabling extended producer responsibility (EPR) programs.

The implementation of DPPs depend on interconnected digital systems like cloud platforms, APIs, IoT devices, and blockchain networks, thus, DPPs and their infrastructure are exposed to the security weaknesses inherent in these technologies.

Threats to DPP data
Unauthorized access/data breaches: Intruders or malicious insiders can access confidential design or compliance information.

Data manipulation and tampering: Unauthorized changes to environmental data by malicious actors , such as falsifying carbon emission figures.

Data loss and ransomware: Operational shutdowns caused by data being deleted or encrypted by ransomware.

Data leakage/oversharing: Unintended exposure of sensitive business information or personal data protected under GDPR.

Replay/cloning attacks: Fraudulent replication of authentic DPPs to market counterfeit goods.

Threats to DPP Infrastructure
Denial of Service (DoS) and ransomware: Attacks that disrupt DPP registries or verification services.

API and integration vulnerabilities: Exploits resulting from weak authentication or insufficient input validation.

Identity and authentication attacks: Phishing, credential theft, and forgery of digital signatures.

Supply chain/software risks: Security gaps introduced through compromised third party components or APIs.

Blockchain specific risks: Vulnerabilities such as smart contract flaws, Sybil attacks, or 51% attacks.

Security measures and best practices data protection strategies
Encryption: Using AES-256 or any other quantum resistant encryption algorithm for stored data and TLS for data being transferred.

Access control: Implementing role based access control (RBAC), the principle of least privilege, and multi-factor authentication (MFA).

Data integrity: Ensuring data authenticity with digital signatures, cryptographic hashing, and blockchain or Merkle-tree verification.

Auditability: Maintaining immutable logs with timestamps to track all changes.

Lifecycle management: Applying secure data deletion or archiving rules for DPPs that are no longer active.

Infrastructure security strategies
DDoS protection: Deploying Web Application Firewalls (WAFs), rate limiting, and redundant systems.

API security: Using OAuth2, JWT tokens, strict input validation, and abuse detection.

Secure development lifecycle (SDLC): Conducting regular vulnerability scans, penetration tests, and third-party code audits.

Supply chain security: Performing rigorous vendor security checks and monitoring software bill of materials (SBOM).

Compliance and governance
Security for DPPs is fundamentally linked to regulatory compliance. Organizations must align with:

GDPR: For the protection of personal and sensitive business data.

NIS2 directive: For ensuring the resilience of essential digital infrastructure.

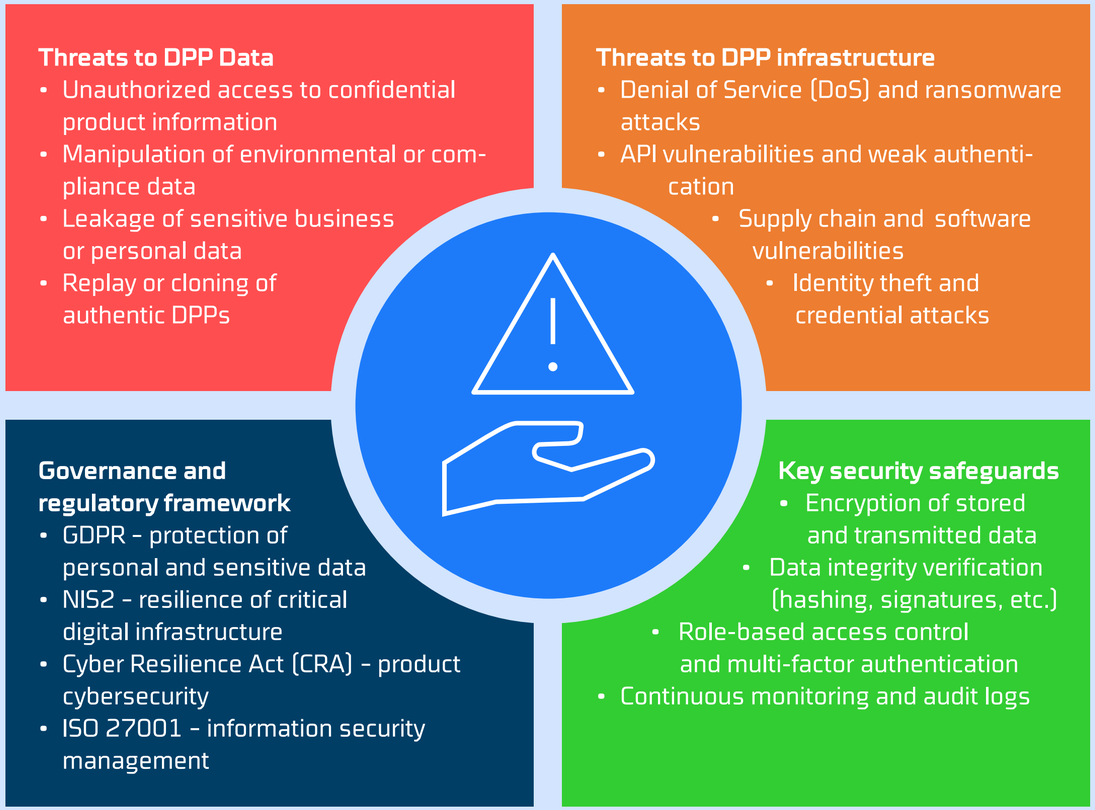
Ecodesign for Sustainable Products Regulation (ESPR): Which sets the mandatory requirements for DPPs.

ISO 27001 Frameworks: Providing established standards for information security management.

Governance frameworks must clearly outline data ownership, stewardship responsibilities, and obligations across the supply chain. Furthermore, Service Level Agreements (SLAs) and Data Processing Agreements (DPAs) should require all partners to adhere to DPP security standards.

Risk management and incident response
A proactive approach to risk management is essential. This involves creating an incident response plan (IRP) specific to DPP systems, which includes:

- Modeling threats like insider fraud, counterfeiting, and data corruption.
- Implementing real time monitoring using Security Information and Event Management (SIEM) tools.
- Conducting regular backup and disaster recovery tests.
- Fostering continuous improvement through security audits, tracking key performance indicators (KPIs), and applying lessons learned from past incidents.



5 actions companies can take regarding the Digital Product Passport

Based on the insights outlined in this report, companies can already begin taking meaningful steps to prepare for the requirements of the DPP. The material highlights that several foundational activities can be initiated now because they rely on existing data, processes, and organizational structures. Together, these actions provide a practical starting point for building the capabilities, governance, and technological readiness that will later be essential for full DPP compliance. This early focus enables organizations to reduce future implementation risks, strengthen internal alignment, and accelerate their overall digital and sustainability transformation.

1. Map existing product and material data
Companies should conduct a structured data mapping exercise across existing product data systems, including ERP, PIM, PLM, and supplier platforms.

The objective is to establish visibility into:
- What data already exists
- Where it is stored
- Who owns it
- The current level of data quality

This exercise is independent of the delegated acts and can significantly reduce future implementation timelines.

2. Assess and strengthen data quality and governance
The Digital Product Passport will require consistent, reliable, and verifiable data.

Companies can already:
- Conduct sample based data quality assessments
- Identify data gaps and inconsistencies
- Define internal data ownership roles and governance structures
- Improved data quality provides immediate operational benefits and will accelerate future compliance efforts.

3. Analyze internal and external data flows
Organizations should review both their internal data logistics and how data is exchanged with customers, suppliers, and other stakeholders.

This includes:
- Integration between ERP and other enterprise systems
- Identification of manual processes
- Assessment of interoperability readiness

This analysis lays the foundation for a future ready system architecture.

4. Evaluate and pilot relevant data carrier technologies
Companies can start exploring different options of data carriers (e.g., QR codes, NFC, RFID). Some already mentioned earlier.

Companies can:
- Test durability and technical performance
- Assess integration with existing systems
- Analyze operational side benefits such as inventory optimization and traceability

This represents a low-risk investment with potential operational upside.

5. Anchor DPP strategically within the organization
The Digital Product Passport should not be treated as a standalone compliance initiative, but as part of a broader digital and sustainability transformation strategy.

Companies can:
- Appoint an internal project lead
- Integrate DPP into existing ESG and digital transformation programs
- Ensure executive-level sponsorship

Early organizational alignment reduces implementation risk and strengthens decision-making.

AUTHORS

Meiken Hansen
Senior Consultant
mnha@forcetechnology.com

Jasmin Nicolaisen Skøtt
Innovation Consultant
mnha@forcetechnology.com

Sofie Fiora Milstjerne
Digital Innovation Lead
sai@forcetechnology.com

Ahmed Khan Leghari
Senior Specialist
ahkl@forcetechnology.com

Rasmus Reeh
Chief Consultant
rre@forcetechnology.com

Asger Norlund
Senior Specialist
asno@forcetechnology.com

FORCE Technology
Park Allé 345
2605 Brøndby
Danmark
+45 43 25 00 00
info@forcetechnology.com
forcetechnology.com

62301