zvei
electrifying ideas

Der Digitale Produktpass

Herausforderungen bei Einführung, Skalierung und Cybersicherheit des DPP

Verband der Elektro- und Digitalindustrie

1. Einleitung

Mit dem Digitalen Produktpass (*Digital Product Passport, DPP*) verfolgt die Europäische Union das Ziel, durchgängige Transparenz über Produkte entlang ihres gesamten Lebenszyklus zu schaffen – von der Herstellung über die Nutzung bis zur Entsorgung oder Wiederverwendung. Als zentrales Instrument der Ökodesign-Verordnung für nachhaltige Produkte (*Ecodesign for Sustainable Products Regulation*, ESPR) soll der DPP die Grundlage für fundierte Entscheidungen von Verbraucher:innen, Marktakteuren und Behörden liefern. Das übergeordnete Ziel ist es, Ressourceneffizienz, Nachhaltigkeit und Kreislaufwirtschaft substanziell zu stärken.

Was als einfaches Instrument zur digitalen Bereitstellung von Produktinformationen angekündigt wurde, hat sich in kürzester Zeit zu einem komplexen regulatorischen, technischen und organisatorischen Vorhaben entwickelt. Seit dem Kommissionsvorschlag aus dem Jahr 2022 wird an einem System gearbeitet, bei dem ein digitales Registry-System, dezentrale Datenquelle, interoperable Schnittstellen und eine Vielzahl potenzieller Zugriffs- und Nutzungsszenarien Berücksichtigung finden müssen. Die Vielzahl von Stakeholdern – vom Regulator über Produkthersteller und Service Provider hin zu Kunden und Nutzern, Wartungsbetrieben und Recyclern – und die jeweiligen Anforderungen an das DPP-System tragen zur Komplexität des Gesamtsystems bei.

Die Einführung des DPP wird produzierende Industrien Europas über deren Wertschöpfungsstufen hinweg betreffen. DPPs werden verpflichtend werden für alle Produkte, die unter die ESPR fallen. Prinzipiell betrifft dies Produkte im europäischen Binnenmarkt, einschließlich Bauteile und Zwischenprodukte. Zunächst greift die Produkt-Priorisierung des 1. ESPR Working Plans, darunter sind auch „Energy-related products“ und „ICT products“ erfasst. Es gibt jedoch noch weitere EU Regularien, die sich auf einen DPP beziehen (u.a. Batterieverordnung). Die Umsetzung des DPP erfordert Investitionen in IT-Infrastruktur, Prozessanpassungen, neue Datenmodelle sowie verbindliche Rollen- und Rechtekonzepte. Unternehmen sollen DPPs bereitstellen, aktuell halten, zugänglich machen, archivieren, absichern und das millionenfach, auch für Produkte mit kurzer Lebensdauer, niedrigem Risiko oder geringem wirtschaftlichem Wert.

Das DPP-System soll 2027 ausgerollt werden. Dazu sind zentrale Umsetzungsfragen, wie etwa klare Vorgaben zur Datensensibilität, zur Cybersecurity, zur Ausfallsicherheit, zu Backup- und Archivierungspflichten oder zu akzeptablen Service Levels, zu klären. Es fehlen operative Leitlinien für die Systemintegration, insbesondere für kleine und mittlere Unternehmen (KMU), ebenso wie realistische Zeitpläne für die Einführung über unterschiedliche Sektoren hinweg.

Um die weitreichenden Ziele der Europäischen Gesetzgeber in Bezug auf die Förderung von Nachhaltigkeit, Wettbewerbsfähigkeit und Innovation in Europa zu erreichen, wird ein zukunftsfähiges DPP-System benötigt, welches neben verpflichtenden regulatorischen Minimalanforderungen auch die Möglichkeit auf freiwilliger Basis digitale Geschäftsmodelle ermöglicht. Um dies in tragbare Weise umzusetzen, gibt es aktuell aus Sicht der Industrie technische und organisatorische Herausforderungen des DPP-Systems, die in diesem Whitepaper adressiert werden . Dabei geht es nicht um die Inhalte der produktbezogenen Daten, sondern ausschließlich um den Aufbau, Betrieb und die langfristige Tragfähigkeit des DPP-Gesamtsystems.

2. Grundprinzipien und aktueller Stand des DPP-Systems

Zielbild und Funktionsweise des Digitalen Produktpass (DPP)

Der Digitale Produktpass ist ein zentrales Instrument der europäischen Nachhaltigkeitspolitik im Rahmen des Green Deal und der Kreislaufwirtschaftsstrategie der EU. Als digitale Schnittstelle zwischen Produkten, Märkten und regulatorischen Anforderungen soll er verlässliche Informationen über nachhaltigkeitsrelevante Eigenschaften von Produkten über ihren gesamten Lebenszyklus hinweg bereitstellen. Dies umfasst unter anderem Daten zur Zusammensetzung, zur Energieeffizienz, zur Reparierbarkeit, zur Wiederverwendbarkeit, zur Recyclingfähigkeit und zur Konformität mit regulatorischen Anforderungen.

Das grundlegende Ziel des DPP ist es, Transparenz für Verbraucher:innen, Marktakteure, Recycler und Behörden zu schaffen, um nachhaltige Entscheidungen in Bezug auf Produktanwendung, Reparatur, Wiederverwendung, Recycling und Rücknahme und die Marktüberwachung effizient und datenbasiert zu ermöglichen. Perspektivisch soll der DPP eine *Single Source of Truth* sein, um regulatorisch geforderte Informationen digital, maschinenlesbar und interoperabel bereitzustellen.

Das DPP-System basiert auf folgenden Prinzipien:

- **Dezentrale Datenhaltung:** Die produktbezogenen Informationen werden nicht zentral gespeichert, sondern verbleiben beim Hersteller – in einem firmeneigenen System oder bei einem beauftragten DPP-Dienstleister. Über eine eindeutige Kennung auf dem Produkt (z. B. ein QR-Code) wird auf den dazugehörigen DPP in der jeweiligen Datenquelle verwiesen.

- **Zentrale Registrierung:** Ein zentrales EU-DPP-Register (*Registry*) soll Grundlage für den Zugriff von Verbrauchern, Marktüberwachung, Rückverfolgbarkeit und Versionsmanagement sein.

- **Verteilte Rollen:** Die Akteure übernehmen verschiedene Rollen. Der Zugriff auf Informationen erfolgt nach definierten Zugriffsrechten, z. B. öffentlich, für Marktaufsichtsbehörden oder nur intern.

- **Interoperabilität durch offene Standards:** Damit der DPP in der gesamten EU und über alle Produktgruppen hinweg funktioniert, sind standardisierte Datenformate und Schnittstellen (APIs) erforderlich. Die im DPP enthaltenen Informationen selbst werden sektor- oder produktgruppenspezifisch durch delegierte Rechtsakte definiert.

Der DPP soll technologieneutral sein: Ob ein Unternehmen Daten aus einem ERP-System bereitstellt, einen Cloud-Service nutzt oder eine XML-Datei auf einer Website veröffentlicht, bleibt, innerhalb regulatorischer Grenzen, offen. Genau diese Offenheit bringt jedoch erhebliche Herausforderungen mit sich, wie die weiteren Kapitel zeigen werden.

Vom Konzept zur Umsetzung: Ein fragmentierter Prozess

Obwohl die Ziele des DPP breit kommuniziert und politisch gesetzt sind, befindet sich die technische und organisatorische Umsetzung noch in einem frühen Stadium.

Zentrale Herausforderungen des aktuellen Umsetzungsstandes:

- **Fehlende technische Anforderungen** in den Bereichen Cybersecurity, Datensicherung, Aufbewahrungspflichten, Reaktionszeiten der beteiligten IT-Systeme (Service Levels) und zum System-Deployment (Systemeinführung, -implementierung and -aktualisierung).

- **Fehlende technische Spezifikationen:** Es existieren bislang keine vollständigen, stabilen und konsolidierten technischen Implementierungsspezifikationen. Die ersten Vorschläge zu Architektur, Schnittstellen und Zugriffsrechten befinden sich in informellen Arbeitsdokumenten oder frühen Konzeptpapieren.

- **Fehlende Systemverantwortung:** Es ist derzeit nicht eindeutig geregelt, welche Organisation welche Rolle im DPP-System übernimmt, insbesondere im Hinblick auf:

  – Zertifizierung und Aufsicht über DPP-Serviceprovider
  – Verantwortlichkeit bei Sicherheitsvorfällen, Systemausfällen oder Datenverlust
  – Rechtliche Haftung bei fehlerhaften oder manipulierten DPP-Daten

- **Widersprüchliche Anforderungen an Datenverfügbarkeit und Datenschutz:** Der DPP soll einerseits umfassend informieren, andererseits keine sensiblen oder wirtschaftlich kritischen Informationen enthalten. Die Abgrenzung zwischen öffentlich zugänglichen, eingeschränkt sichtbaren und „vertraulichen“ Informationen ist bislang nicht klar definiert, ebenso wenig wie Schutzmaßnahmen oder Rollenverteilungen für sensible Daten.

Für die Industrie bedeutet dies, dass sie aktuell mit einem System planen muss, dessen Rahmenbedingungen weder technisch noch organisatorisch fixiert sind. Dies führt zu erheblichen Investitionsrisiken, insbesondere bei kleinen und mittleren Unternehmen, die nur begrenzte Kapazitäten für IT-Architektur, Datenschutz, Cybersicherheit und Regulierungs-Compliance aufbringen können.

Fehlende Einführungsszenarien: Ein Risiko für Skalierung und Vertrauen

So ambitioniert das Zielbild des Digitalen Produktpasses ist, so wichtig ist nun ein klar abgestimmtes und praktikables Vorgehen für seine schrittweise Einführung. Der Hochlauf sollte sektoral erfolgen, um Erfahrungen aus einzelnen Bereichen gezielt zu nutzen und das System schrittweise in der Breite des europäischen Markts zu etablieren. Dabei wäre genau das jetzt entscheidend, um Orientierung und Investitionssicherheit zu schaffen.

Zwar ist vorgesehen, dass der DPP in mehreren produktbezogenen Rechtsakten eingeführt wird, doch die technischen, organisatorischen und regulatorischen Grundlagen dafür sind bislang nicht ausgereift. Gleiches gilt auch für den Batteriepass (Battery Passport), der ab 2027 im Rahmen der Batterieverordnung eingeführt wird. Es gibt weder verlässliche Informationen darüber, wie der Betrieb des EU-DPP-Registers organisiert wird, noch wie Unternehmen den DPP in ihre bestehenden Systeme integrieren sollen. Auch Übergangsregelungen, Zertifizierungsverfahren für DPP-Serviceanbieter oder verbindliche Zeitpläne fehlen bislang völlig.

Diese Unsicherheit führt zu erheblichen Risiken für alle Beteiligten: Unternehmen sehen sich gezwungen, mit unvollständigen Vorgaben zu planen, während IT-Dienstleister in einem regulatorischen Vakuum agieren. Gerade KMU haben nicht die Ressourcen, um auf flexible, dynamisch

wachsende Anforderungen mit agilen IT-Projekten zu reagieren. Ohne Planungssicherheit droht ein Flickenteppich an Insellösungen, die langfristig nicht interoperabel sind.

Ein zukunftsfestes System muss jedoch genau das leisten: Koordinierte Einführung, klare Versionierung und transparente Roadmaps. Was derzeit fehlt, ist ein realistisches Rollout-Szenario – auch in technischer Hinsicht. Wie kann der DPP in der Übergangszeit rechtssicher und einfach implementiert werden? Wie wird mit Systemausfällen, Updates und Migrationsfällen umgegangen? Und wie bleiben alle Beteiligten synchron, wenn sich Anforderungen verändern?

Was jetzt gebraucht wird, ist kein vollständig entwickeltes Bild, sondern ein realisierbarer Einstiegspfad mit klaren Zuständigkeiten, technischer Stabilität und regulatorischer Orientierung. Dieser würde Unternehmen erlauben, erste zukunftssichere Schritte zu gehen und gleichzeitig ein belastbares Testfeld schaffen, auf dem Infrastruktur, Schnittstellen und Governance erprobt und weiterentwickelt werden können. Ohne diesen Pfad droht ein Vertrauensverlust sowohl gegenüber dem DPP-System als auch gegenüber der digitalen Transformationspolitik Europas insgesamt.

3. Technische und organisatorische Herausforderungen

3.1. Cybersecurity

Mit der Einführung des Digitalen Produktpass entsteht ein neues, großflächiges, digitales System, das Millionen von Produktpässen über Unternehmens-, Länder- und Sektorgrenzen hinweg zugänglich macht. Damit werden nicht nur produktbezogene Daten digitalisiert, sondern eine hochgradig vernetzte europäische Dateninfrastruktur aufgebaut. Für ein solches System ist Cybersicherheit keine Randbedingung, sondern ein zentrales Strukturmerkmal.

Zentral ist hierbei die Architektur des DPP-Systems: Sie basiert auf dezentraler Datenhaltung und einem zentralen europäischen Register mit offenen Schnittstellen sowie unterschiedlichen Rollenmodellen, die jeder Teilnehmer realisieren muss. Aus Sicht der Industrie ergibt sich daraus eine Reihe kritischer Risikofaktoren, die bislang weder regulatorisch noch technisch ausreichend adressiert sind.

Angriffspotenzial und Bedrohungslage

Der potenzielle Angriffsvektor eines solchen Systems ist enorm, nicht zuletzt aufgrund der Vielzahl der beteiligten Akteure und der potenziellen Nutzbarkeit durch die Öffentlichkeit. Anspruchsvoll ist die Tatsache, dass das System für verpflichtende Angaben zur Konformität des Produktes sowie Informationen zu den Wirtschaftsakteuren , weitgehend durchgängig online verfügbar sein muss. Diese Anforderung ist für den erfolgreichen Übergang zu digitalen Produktinformationen zentral, erhöht jedoch gleichzeitig die Angriffsfläche und die Anforderungen an die IT-Sicherheit erheblich. Es bedarf daher angemessener technischer Maßnahmen, um die Verfügbarkeit sicherzustellen und gleichzeitig Risiken oder unbefugte Manipulationen zu minimieren.

Zentrale Bedrohungen sind unter anderem:

- Denial-of-Service (DoS) und Distributed Denial-of-Service (DDoS)-Angriffe auf das EU-DPP-Register, die den Zugriff auf gesetzlich vorgeschriebene Informationen verhindern. Dies könnte

den freien Warenverkehr bei Zollkontrollen behindern oder die Markteinführen neuer Produkte verzögern.

- Manipulation von DPP-Daten (z. B. Änderung der Konformitätsinformationen oder Produktherkunft), die zu Marktverboten oder Rückrufen führen könnten.
- Gefälschte Registrierung von Marktakteuren, etwa durch unzureichend geschützte Zugangssysteme, mit dem Ziel, unautorisierte oder manipulierte DPPs zu erzeugen.
- Indirekte Wirtschaftsspionage, z. B. durch Auswertung öffentlich abrufbarer Pässe zur Ableitung von Produktionsvolumina, Lieferketten oder Marktanteilen.

Diese Risiken betreffen nicht nur zentrale EU-Infrastrukturen wie Registry und Portal, sondern auch die zahlreichen dezentralen Systeme, die von Unternehmen oder Dienstleistern betrieben werden. Besonders gefährdet sind dabei kleinere Unternehmen, die weder über umfangreiche IT-Sicherheitsressourcen noch über Erfahrung mit dem Betrieb öffentlich exponierter Webdienste verfügen. Um solche Risiken zu minimieren, werden gegenwärtig Lösungen für europäische harmonisierte Normen erarbeitet um u.a. die Vertraulichkeit von Daten, das Management von Zugriffsrechten oder die Authentifizierung von Daten sicherzustellen. Jedoch muss sich auch die Europäische Kommission in dieser Diskussion beteiligen, insbesondere bezüglich der Frage des Risikos bei zentralen EU-Infrastrukturen.

Vertraulichkeit und wirtschaftlich sensible Informationen

Ein grundlegender Zielkonflikt im DPP-System betrifft die Frage der Datensensibilität. Einerseits soll der DPP Transparenz schaffen und möglichst viele Informationen öffentlich bereitstellen. Andererseits enthalten die Daten je nach Branche potenziell vertrauliche oder geschäftskritische Informationen, etwa zu Lieferketten oder Produkteigenschaften.

Wichtig ist daher die Bereitstellung verpflichtender Daten auf einer Need-to-know-Basis. Für Produkte, die unter die Ecodesign for Sustainable Product Regulation (ESPR) fallen, sind die konkreten Anforderungen für einzelne Produktgruppen bisher unklar, da bislang noch keine delegierten Rechtsakte hierzu erarbeitet wurden. Dadurch bietet der derzeitige Rechtsrahmen keine präzise Definition, welche Informationen konkret bereitgestellt werden müssen oder ob diese als zugriffsgeschützt oder sensibel gelten. Damit gibt es auch keine konkreten Vorgaben, wie diese Daten vor unberechtigten Zugriff geschützt werden können. Die Folge: Unternehmen wissen heute nicht, ob sie besonders schützenswerte Informationen überhaupt in den DPP aufnehmen dürfen oder müssen.

Für die Erweiterung des DPP auf andere Rechtsakte dürfen nur Daten, die in den das Produkt betreffenden Rechtsakten als Pflichtangeben vorgesehen sind, für den DPP verpflichtend gefordert werden. Vertrauliche Daten, die nur auf begründetes Verlangen der zuständigen Marktüberwachungsbehörde zur Verfügung gestellt werden müssen, sind weiterhin entsprechend zu behandeln. Darüber hinaus sollte es dem Hersteller freistehen, zusätzliche Daten freiwillig bereitzustellen.

Die Elektro- und Digitalindustrie vertritt daher eine klare Position:

- Der DPP darf im öffentlich zugänglichen Teil keine vertraulichen oder wettbewerbskritischen Informationen enthalten. Sensible Daten, die ausschließlich für bestimmte Behörden oder berechtigte Akteure von Relevanz sind, sollten nur auf begründetes Verlangen bereitgestellt werden.

Darüber hinaus steht es Unternehmen frei, ergänzende Informationen über die gesetzlichen Anforderungen hinaus zur Verfügung stellen. Für die öffentlich zugänglichen Informationen darf ein möglicher Verlust oder eine Veröffentlichung nur ein akzeptables Risiko darstellen.

- Wo Zugriffsbeschränkungen erforderlich sind (z. B. für Marktaufsichtsbehörden), müssen sie rechtlich klar definiert und technisch abgesichert sein.Besonders sensibel ist der Umgang mit direkten Anfragen von Behörden. Hierbei sollte es in der Verantwortung des Herstellers bleiben, diese Anfragen ganz oder teilweise über das DPP-System mit entsprechenden Zugriffsberechtigungen abzuwickeln oder über andere abgesicherte Kanäle mit nachvollziehbarem Legitimitätsnachweis und nachvollziehbarer Veranlassung zu nutzen.

Identitäten, Rollen und Zugriffskontrolle

Ein weiteres Thema für die Sicherheit des DPP-Systems ist das Identitäts- und Zugriffsmanagement. Es stellen sich folgende Fragen:

- Wie werden Identitäten und Anmeldedaten (Nutzernamen, Passwörter, Zertifikate u.ä.) für die Vielzahl von Teilnehmern im DPP-System erstellt, an Organisationseinheiten weitergegeben und aktuell gehalten?
- Wer darf DPPs erstellen? Wer darf sie ändern? Wer trägt die Verantwortung für die DPP-Inhalte?
- Wer darf DPPs einsehen und mit welchem Umfang?

Im bisherigen Systemdesign ist vorgesehen, dass Unternehmen verschiedene Rollen einnehmen können – als Hersteller, als Händler, als Serviceanbieter. Doch in der Praxis sind diese Rollen nicht eindeutig trennbar: Ein Unternehmen kann gleichzeitig Hersteller eigener Produkte, Betreiber von Kundenanlagen, Importeur von Komponenten und After-Sales-Dienstleister sein, oft mit unterschiedlichen Teams, Standorten oder sogar Gesellschaften.

Hinzu kommen internationale Konstellationen mit Betriebsstätten innerhalb und außerhalb der EU. Die Verwaltung von Rollen und Zugriffsrechten wird dadurch zu einer komplexen organisatorischen Aufgabe mit hohen Anforderungen an interne Governance und an technische Schnittstellen.

Die Elektro- und Digitalindustrie fordert daher, dass die EU ein allgemeines Rahmenwerk für Identitäts- und Rollenmanagement im DPP-Kontext entwickelt.

Dazu gehören:

- Einheitliche Verfahren zur Registrierung von Marktakteuren (z. B. über EU-Login)
- Klare Rollendefinitionen und Zuordnung von Rechten
- Minimalistische Ansätze für den öffentlichen Zugriff (nur lesend, keine Interaktionen)
- Möglichkeit zur dezentralen Verwaltung von Unternehmensrollen (z. B. durch Hersteller-Admin, Supplier-Reader etc.), wie im EPREL-System bereits realisiert.

Dieser Rahmen sollte allgemein ausgestaltet und dann je Produktsektor angepasst sein.

Sicherheitsanforderungen an das Systemdesign

Aus technischer Sicht steht das DPP-System vor der Herausforderung, ein offenes, interoperables und gleichzeitig sicheres System zu realisieren. Eine solche Architektur ist nicht trivial, insbesondere, wenn sie über tausende Systeme hinweg funktionieren muss.

Wesentliche Anforderungen aus Sicht der Elektro- und Digitalindustrie:

- **Security by Design:** Sicherheitsanforderungen dürfen kein Add-on, sondern müssen integraler Bestandteil des Systemdesigns sein – insbesondere bei Schnittstellen, Authentifizierung, Verschlüsselung und Protokollen.
- **Reduzierung der Angriffsfläche:** Nur Daten, die in den das Produkt betreffenden Rechtsakten als Pflichtangaben vorgesehen sind, dürfen für den DPP verpflichtend gefordert werden. Zusätzlich können Unternehmen freiwillig weitere Daten öffentlich bereitstellen.
- **Klare Trennung von öffentlichem und nicht-öffentlichem DPP-Bereich:** Zwei technisch und organisatorisch getrennte Zugriffsebenen mit Rollenkonzept.
- **Niedrige Betriebsanforderungen für dezentrale Systeme:** Das Hosting eines DPP-Links darf nicht bedeuten, dass ein Unternehmen eine hochverfügbare Server-Infrastruktur oder einen 24/7-Support betreiben muss. Auch sollten die Anforderungen an Zugriffszeiten und Verfügbarkeit nicht wesentlich über die an heutige Firmen-Portale hinausgehen.
- **Vermeidung von Single Points of Failure:** Zentrale DPP-Dienste wie die EU-DPP-Registry oder das System für das Management von Identitäten und Zugangsdaten dürfen nicht zum Flaschenhals werden, weder in Bezug auf Zugriff noch auf Sicherheitsvorfälle.

Wir sprechen uns ausdrücklich dafür aus, dass DPP-relevante Informationen nicht an geschäftskritische Prozesse gekoppelt werden. Ein temporärer Ausfall eines DPP-Links darf keine Marktblockade oder Verzögerung in der Lieferkette verursachen.

3.2. Datenhaltung und Backups

Ein bislang weitgehend ungelöstes Problem im Kontext des DPP ist die Frage der langfristigen Datenhaltung und Sicherung. Zwar entsteht mit dem DPP ein neues Instrument zur strukturierten Produktdatennutzung, doch die regulatorischen Rahmenbedingungen zur Archivierung, Datensicherung und Wiederverfügbarkeit sind bislang vage oder nicht vorhanden.

Die ESPR fordert zwar, dass mit Inverkehrbringen des Produkts neben dem DPP auch ein Back-Up des DPP durch einen unabhängigen Service-Dienstleister zur Verfügung gestellt wird, sie enthält jedoch keinerlei verbindliche Aussagen zu damit verbundenen Backup-Pflichten oder Aufbewahrungsfristen für DPP-Daten. Auch für den Fall von Unternehmensinsolvenzen, Übernahmen, Fusionen oder dem Ende von Produktlebenszyklen existieren keine klaren Anforderungen oder Prozesse. Gleichzeitig entstehen durch die systemische Architektur des DPP neue Verantwortlichkeiten für Unternehmen, die im Zweifel umfangreiche und redundante Backup-Systeme aufbauen müssten – ohne rechtliche Klarheit, wer in welchem Fall zur Datensicherung verpflichtet ist.

Diese Unsicherheit birgt erhebliche Risiken. So wäre eine verpflichtende Sicherung aller DPPs, inklusive aller referenzierten Dokumente wie Handbücher, Konformitätserklärungen oder Recyclinginstruktionen, mit sehr großen Datenvolumina verbunden. Der Aufbau entsprechender

Archivstrukturen wäre insbesondere für KMU weder verhältnismäßig noch wirtschaftlich tragfähig. Auch die Forderung, dass DPPs über das Ende eines Unternehmens hinaus erhalten bleiben sollen, erscheint unverhältnismäßig und wirft Fragen nach der Finanzierung auf.

Es ist unklar, wie die langfristige Gültigkeit digitaler Signaturen und Datenformate sichergestellt werden soll, insbesondere bei sich ändernden Standards, Unternehmen oder Technologien.

In der industriellen Praxis gilt heute ein anderer Grundsatz: „Wer Daten benötigt, trägt Verantwortung für deren Sicherung." So unterliegen Betreiber kritischer Anlagen oder Maschinen der Pflicht, relevante Produktinformationen lokal vorzuhalten, um im Falle externer Ausfälle handlungs- und auskunftsfähig zu bleiben. Dieses Prinzip sollte auch im DPP-Kontext gelten. Die Archivierung aller DPPs über Jahrzehnte durch Hersteller oder Service-Provider wäre weder notwendig noch sinnvoll, insbesondere nicht für kurzlebige Konsumgüter.

Der Vorschlag der Elektro- und Digitalindustrie lautet daher: Die EU sollte einen klaren allgemeinen Rahmen zur Datenhaltung und Datensicherung im DPP-System schaffen, etwa durch horizontal geltende Prinzipien zur Zuständigkeit und Aufbewahrungsdauer. Branchenspezifische Anforderungen sollten dann durch sektorale delegierte Rechtsakte präzisiert werden. Nur so lassen sich überzogene Anforderungen vermeiden und gleichzeitig sicherstellen, dass Daten dort vorgehalten werden, wo sie tatsächlich gebraucht werden: praxisnah, verhältnismäßig und rechtssicher.

3.3. Service Levels

Ein wichtiger, aber bisher unterschätzter Aspekt in der Ausgestaltung des DPP ist die Frage nach der Systemverfügbarkeit und den erwarteten Reaktionszeiten – den Service Levels. Während in der politischen Diskussion oft die umfassende Verfügbarkeit digitaler Produktinformationen betont wird, fehlt bislang eine realistische Einschätzung dessen, wie hoch die Anforderungen an die Verfügbarkeit tatsächlich sein sollten und welche Konsequenzen diese für Infrastruktur, Betriebskosten und regulatorische Abhängigkeiten hätten.

Aus Sicht der Industrie ist klar: Die Service Levels eines DPP-Systems müssen sich an der realen Nutzung und Bedeutung der Daten orientieren. Produktinformationen wie Nachhaltigkeitsmerkmale, Entsorgungshinweise oder Konformitätsangaben sind wichtig, aber ihr Abruf ist in der Regel nicht zeitkritisch. Ob man eine Ökodesign-Kennzahl oder eine Recyclinganleitung in Sekunden oder Minuten erhält, hat meist keine unmittelbaren Auswirkungen auf den Geschäftsbetrieb oder auf die Produktsicherheit.

Dennoch birgt die aktuelle Unsicherheit das Risiko der Überdimensionierung: Würden an das DPP-System dieselben Anforderungen gestellt wie an geschäftskritische Systeme (z. B. für Zahlungsverkehr oder Logistiksteuerung), wären hochverfügbare Infrastrukturen mit massiven Investitions- und Betriebskosten, insbesondere für kleinere Anbieter, erforderlich.

Hier ist politische Klarheit erforderlich: Der DPP sollte für verpflichtende Informationen als Informationssystem begriffen werden, dessen Daten zwar wichtig, aber in ihrer Nutzung nicht zeitkritisch sind. Unternehmen haben jedoch die Möglichkeit, zusätzliche Informationen freiwillig bereitzustellen und so den Nutzen des DPP für eigene Zwecke oder Partner zu erweitern.

Die Lösung liegt in einer gestuften Service-Level-Strategie:

- **Für die allgemeine Nutzung,** etwa durch Verbraucher, Reparaturdienste oder Entsorger, sind moderate Service Levels in der Regel ausreichend und eine zeitweise eingeschränkte Verfügbarkeit stellt oftmals kein regulatorisches Problem dar. Für besonders relevante Informationen, etwa zur Inbetriebnahme oder Sicherheitsangaben, muss jedoch sichergestellt werden, dass diese zuverlässig bereitgestellt werden, da andernfalls Haftungsrisiken für Hersteller entstehen könnten.
- **Für Behördenzugriffe (z. B. Marktüberwachung)** ist sicherzustellen, dass mittel- bis langfristig auf die benötigten Informationen zugegriffen werden kann, etwa durch Zwischenspeicherung oder andere Absicherungen.
- **Für Unternehmen** gilt der Grundsatz: Der DPP darf keine unternehmenskritischen Prozesse blockieren. Zahlungen oder Lieferfreigaben dürfen nicht von einer Echtzeitverfügbarkeit der DPP-Infrastruktur abhängig gemacht werden.

Die Elektro- und Digitalindustrie fordert deshalb: Die EU sollte in der Umsetzung des DPP Service Level so formulieren, dass diese realistisch den Anforderungen an die Prozesse sind. Nur mit einer realistischen, nutzungsorientierten Service-Level-Politik kann der DPP langfristig kosteneffizient betrieben und breit akzeptiert werden.

3.4. Systemeinführung, Betrieb und Aktualisierung, Skalierung

Die Einführung des DPP ist nicht nur ein inhaltliches und rechtliches großes Vorhaben, sondern vor allem eine beispiellose organisatorische und technische Herausforderung. Die Vision eines interoperablen, sektorübergreifenden Systems mit Milliarden registrierten Produkten, tausenden beteiligten Akteuren und dezentraler Datenhaltung erfordert eine präzise, koordinierte und mehrstufige Umsetzung. Bisher bleibt offen, wie diese Umsetzung konkret gelingen soll. Ein Risiko, das die gesamte Wirkungskraft des DPP gefährdet.

Eine fragmentierte Systemlandschaft

Bereits heute ist absehbar, dass sich der DPP in eine hochgradig heterogene IT-Landschaft integrieren muss:

- Rund 2,2 Millionen europäische Unternehmen, darunter viele KMU, werden eigene DPP-Systeme betreiben oder Dienste Dritter nutzen.
- Hinzu kommen Importeure, E-Commerce-Plattformen, Distributoren und andere Akteure außerhalb der EU.
- Zentrale EU-Infrastrukturen wie das DPP-Registry, das Webportal, Systeme der Marktüberwachung und der Zollbehörden müssen eingebunden und stabil betrieben werden.
- All diese Systeme müssen nahtlos interoperieren: technisch, semantisch und rechtlich.

Bereits kleinste Unstimmigkeiten bei Schnittstellen, Datenformaten oder Update-Zyklen können zu massiven Störungen führen.

Risiken durch fehlende Standardisierung und Koordination

Die fehlende Ausreifung zentraler DPP-Komponenten birgt ein Risiko für Fehlinvestitionen. Gleichzeitig fehlen klare Roadmaps, Versionierungsrichtlinien und Migrationspläne, die eine sichere und schrittweise Einführung ermöglichen würden.

Besonders herausfordernd sind Änderungen an Interoperabilitätsstandards oder Schnittstellen: Ohne abgestimmte Roll-out-Pläne, Übergangsfristen und Rückwärtskompatibilität ist jedes System-Update mit hohem Personalaufwand und Risiko bei allen Akteuren verbunden, gleicherweise bei multinationalen Unternehmen mit komplexer IT-Landschaft und Zulieferketten, als auch bei den von der EU betriebenen Systemen.

Ein pragmatischer Vorschlag: Minimum Viable DPP

Die Einführung des Digitalen Produktpasses (DPP) ist ein hochkomplexes Vorhaben mit Milliarden von betroffenen Produkten, Akteuren und Schnittstellen. Ein sofortiger, vollumfänglicher Roll-out birgt erhebliche Risiken: unklare Spezifikationen könnten zu Fehlentwicklungen führen, heterogene IT-Landschaften würden überfordert, und insbesondere kleine und mittlere Unternehmen (KMU) wären mit unverhältnismäßigen finanziellen und organisatorischen Belastungen konfrontiert.

Um diese Risiken zu minimieren und gleichzeitig frühzeitig Nutzen zu stiften, empfiehlt die Industrie – im Einklang mit dem von **Orgalim** vorgeschlagenen Ansatz – eine **stufenweise Einführung** (staged approach) des DPP-Systems. Ziel ist es, in einer ersten Phase die zentralen Funktionen bereitzustellen, die den größten gesellschaftlichen und wirtschaftlichen Mehrwert schaffen, während komplexere Elemente in einer zweiten Phase folgen.

In der ersten Phase sollte zudem ein schlanker, praxisnaher Ansatz gewählt werden, der die frühzeitige Bereitstellung zentraler Informationen ermöglicht, ohne die Unternehmen, insbesondere KMU, mit unnötiger Komplexität zu überlasten. Ein „Minimum Viable DPP“ (MVDPP) sollte folgende Eigenschaften erfüllen:

- In einer Übergangsphase kann die DPP-Bereitstellung direkt über Herstellerwebseiten erfolgen.
- Der DPP enthält ausschließlich nicht-sensible Daten, die öffentlich bereitgestellt werden können – etwa Nachhaltigkeitsinformationen, Produktkennzahlen oder Links auf externe Quellen.
- Die Registrierung erfolgt nur durch verifizierte Wirtschaftsbeteiligte innerhalb der EU.
- Die Datenübertragung erfolgt über einfach strukturierte, stabile Datenformate (z. B. XML), mit klarer Dokumentation und niedriger Einstiegshürde.
- Ein zentrales DPP-Registry-System dient primär der Auffindbarkeit und Verlinkung – nicht der Validierung oder Echtzeitüberwachung.
- Existieren für Produktgruppen bereits etablierte Systeme, die benötigte Produktinformationen zur Verfügung stellen (bspw. die EPREL-Datenbank im Bereich der Hausgeräte), können in der Übergangszeit diese auch für DPP-relevante Informationen genutzt werden. Langfristig sollte eine Interoperabilität dieser Systeme angestrebt werden, um bürokratischen Mehraufwand zu minimieren und Doppelstrukturen für Hersteller zu verhindern. Darüber hinaus können Unternehmen freiwillig zusätzliche Informationen bereitstellen, um den Nutzen des DPP für Nutzer und Partner zu erhöhen.

Erst in späteren Phasen, wenn die technischen Standards ausgereift, die Verwaltungsprozesse etabliert und die Marktteilnehmer vorbereitet sind, kann das System schrittweise ausgebaut werden: Mit feingliedrigeren Rollenmodellen, erweiterten Dateninhalten und stärkeren Validierungsfunktionen.

4. Forderungen an die Politik

Die Einführung des DPP stellt eine bedeutende Weichenstellung für die europäische Industrie dar. In seiner Grundidee, als Instrument zur transparenten Bereitstellung von Nachhaltigkeits- und Konformitätsinformationen entlang der Wertschöpfungskette, bietet der DPP erhebliches Potenzial für eine zirkuläre und resilientere Wirtschaft.

Doch aktuell ist klar: Die Umsetzung des DPP droht an ihrer eigenen Komplexität zu scheitern, wenn nicht rasch realistische Rahmenbedingungen geschaffen werden. Die technische, organisatorische und regulatorische Architektur ist bislang unvollständig und in vielen Punkten intransparent.
Gerade angesichts der ersten verpflichtenden Anwendungsfälle ab 2027 (z. B. Batteriepass) braucht die Industrie verlässliche Leitplanken. Sonst entsteht ein System, das hohe Erwartungen nicht erfüllt, Marktverzerrungen begünstigt und unnötig Ressourcen bindet, insbesondere bei kleinen und mittleren Unternehmen.

Unsere zentralen Forderungen sind deshalb:

1. **Einführung eines Minimum Viable DPP:**
   Für eine Übergangsphase sollte die Zahl der im DPP-System verpflichtend bereitzustellenden Informationen auf das absolut notwendige Maß beschränkt werden. Hersteller sollen die DPPs auf den eigenen Webseiten bereitstellen können, ohne dafür komplexe oder hochverfügbare Infrastrukturen aufbauen zu müssen. Die verpflichtenden Inhalte beschränken sich auf nichtsensible, öffentlich zugängliche Informationen. Darüber hinaus können Unternehmen freiwillig ergänzende Informationen bereitstellen, um den Nutzen des DPP für Anwender und Partner zu erhöhen.
2. **Keine sensiblen oder wirtschaftlich vertraulichen Daten im DPP:**
   Informationen mit Geschäftsrelevanz oder Sicherheitsbedenken dürfen nicht im frei zugänglichen DPP-Teil erscheinen. Zugriff auf weitergehende Informationen sollte ausschließlich kontrolliert, fallbezogen und nachvollziehbar möglich sein – z. B. über begründete Anfragen durch Marktüberwachungsbehörden.
3. **Realistische Anforderungen an Service Levels:**
   Das DPP-System muss Service Level so formulieren, dass diese realistische Anforderungen an die Prozesse stellen. Es darf keine Verpflichtung entstehen, den DPP in unternehmenskritische Prozesse (z. B. Produktauslieferung, Zahlungsabwicklung) zu integrieren.
4. **Klarer regulatorischer Rahmen zu Datenhaltung und Backups:**
   Wer auf Informationen angewiesen ist, trägt die Verantwortung für deren Vorhaltung. Eine generelle Verpflichtung zur vollständigen DPP-Archivierung, über Unternehmensgrenzen und -laufzeiten hinweg, ist unverhältnismäßig. Ebenso wird eine verpflichtende Sicherung über externe DPP-Serviceprovider als problematisch bewertet. Die EU sollte stattdessen einen allgemeinen Rahmen für Datenhaltung und Back-Ups schaffen, der durch sektorale Vorgaben in

den Delegierten Rechtsakten ergänzt wird, um praktikable und verhältnismäßige Lösungen zu gewährleisten.

5. **Rollen- und Zugriffsmanagement vereinfachen:**
   Der Zugriff auf DPP-Informationen sollte durch ein einfaches, rollenbasiertes Berechtigungssystem geregelt werden – zwei Rollen (öffentlich / Marktüberwachung & Kommission) sind ausreichend. Die Verwaltung der Zugriffsrechte soll bei den Herstellern liegen, die ihre Nutzer und Berechtigungen selbst verwalten.
6. **Klare Roadmaps und technische Spezifikationen vorlegen:**
   Die EU-Kommission muss konkrete, abgestimmte Fahrpläne für Systemeinführung, Versionierung und Interoperabilität vorlegen. Ohne stabile Schnittstellen und Standards, und ohne definierte Migrationspfade sind Investitionen und IT-Rollouts in der Breite nicht zu stemmen.

5. Fazit

Die Einführung des DPP ist eine Chance, Europas Wirtschaft nachhaltiger, digitaler und zukunftsfähiger zu gestalten. Der Wandel gelingt, wenn alle beteiligten Akteure gemeinsam an den Lösungen arbeiten und die Weichen stellen. Dazu gehören verlässliche regulatorische Vorgaben ebenso wie technische Grundlagen, die Innovation fördern und den Wandel beschleunigen.

Die Komplexität des DPP-Systems zeigt deutlich, dass technologische Innovation allein nicht ausreicht. Entscheidend ist, dass die Rahmenbedingungen praktikabel gestaltet werden, um nicht unnötig Ressourcen zu binden oder kleinere Marktteilnehmer zu überfordern. Gleichzeitig dürfen Verzögerungen im Aufbau des DPP-Systems nicht zu doppelten Berichtspflichten in Bezug auf digitale Angaben und Angaben in Papierform für Compliance-relevante Informationen bei Unternehmen führen. Nur so entsteht ein Umfeld, in dem der DPP nicht zur administrativen Belastung, sondern zum echten Mehrwert wird.

Die politische Aufgabe besteht daher darin, Balance zu schaffen: zwischen ambitionierten Nachhaltigkeitszielen und den realen Kapazitäten der Wirtschaft; zwischen notwendiger Sicherheit und praktikabler Umsetzung; zwischen Innovation und Verlässlichkeit.

Ein erfolgreiches DPP-System wird dadurch entstehen, dass klare, pragmatische Leitlinien vorgeben, was technisch möglich und wirtschaftlich sinnvoll ist; ohne die Ambitionen zu verwässern. Nur so kann der DPP zu einem Motor für Wettbewerbsfähigkeit, Kreislaufwirtschaft und Vertrauen in europäische Produkte werden. Dies erfordert Mut zu Vereinfachungen, Offenheit für den Dialog mit der Industrie und den Willen, technologische und organisatorische Herausforderungen frühzeitig und gemeinsam zu adressieren.

Kontakt

Angelina Marko • Geschäftsführerin Plattform Digital Ecosystems & Smart Services • Bereich Industrie
Mobil: +49 162 2664-977 • E-Mail: angelina.marko@zvei.org

ZVEI e. V. • Verband der Elektro- und Digitalindustrie • Amelia-Mary-Earhart-Str. 12 • 60549 Frankfurt a. M.
Lobbyregisternr.: R002101 • EU Transparenzregister ID: 94770746469-09 • www.zvei.org

Datum: 23.09.2025