

ESPR Digital Product Passport (DPP) uitdagingen in **implementatie**, **opschaling** en **cybersecurity**

SECTORANALYSE EN WHITEPAPER | PAUL BORGHOUTS & MARLOU SNELDERS



Colofon

FME Zoetermeer, februari 2026

Opgesteld en vertaald door:*

P.T. (Paul) Borghouts (Extern Projectmanager, in opdracht van FME) en
M. (Marlou) Snelders (Policy Advisor Digital en Cyber bij FME)

Zilverstraat 69
Postbus 190, 2700 AD Zoetermeer

+31 (0)79 3531248
+31 (0)6 50651187
paul.borghouts@fme.nl
marlou.snelders@fme.nl

www.fme.nl
www.fme.nl/nl/regelgeving-en-normalisatie

Bronbestand:
DPP industry view 4 december 2025

**Dit document is ontwikkeld op basis van het ZVEI-document 'Industry View on the Digital Product Passport' (<https://www.zvei.org/en/press-media/publications>) en de daarbij horende standpunten van de Duitse elektrotechnische industrie. De analyse, duiding en aanbevelingen zijn vertaald naar de Nederlandse context van FME en haar achterban, met speciale aandacht voor haalbaarheid, proportionaliteit en uitvoerbaarheid voor de technologische industrie.*

Niets uit deze uitgave mag zonder voorafgaande schriftelijke toestemming van de uitgever worden openbaar gemaakt of veeleenvoudigd, waaronder begrepen het reproduceren door middel van druk, offset, fotokopie of microfilm of in enige digitale, elektronische, optische of andere vorm.

Voorwoord

Het Digital Product Passport (DPP) wordt een sleutelement binnen de Europese duurzaamheids- en industrie agenda. Het biedt kansen voor transparantie, circulariteit en efficiëntere waardeketens, maar vraagt tegelijk ingrijpende aanpassingen in databeheer, IT-systemen en organisatieprocessen. Veel onderdelen van het DPP-stelsel zijn nog in ontwikkeling, waardoor bedrijven behoefte hebben aan duidelijke kaders en een realistische invoeringsroute. Zonder duidelijke governance, proportionele servicelevels en juridische duidelijkheid dreigt het Digital Product Passport uit te groeien tot een kostbaar en risicovol verplichtingssysteem in plaats van een instrument ten goede van duurzaamheid en concurrentiekracht.

Dit document is geschreven voor fabrikanten, importeurs, distributeurs, installatiebedrijven, machinebouwers en andere organisaties binnen de Nederlandse technologische industrie, evenals Europese en nationale beleidsmakers en toezichhouders. Het ondersteunt bedrijven in hun voorbereiding op de aankomende verplichtingen en biedt beleidsmakers inzicht in de randvoorwaarden die nodig zijn voor een haalbare en proportionele invoering.

In dit document gebruiken wij de term Digital Product Passport of Digitaal Productpaspoort uitsluitend voor het wettelijk verplichte ESPR-DPP zoals vastgesteld in de Ecodesign for Sustainable Products Regulation. Hiermee doelen wij nadrukkelijk niet op aanvullende of vrijwillige productinformatie die buiten het kader van de ESPR valt.

FME presenteert hiermee een sectoranalyse en positionpaper, waarbij de inhoudelijke analyse en kernargumenten zijn ontleend aan het standpunt van ZVEI en vertaald naar de Nederlandse praktijk.

Paul Borghouts en Marlou Snelders

FME
Februari 2026

*"Zonder duidelijke governance,
proportionele servicelevels en juridische
duidelijkheid dreigt het Digital Product
Passport uit te groeien tot een kostbaar
en risicovol verplichtingssysteem in
plaats van een instrument ten goede van
duurzaamheid en concurrentiekracht"*



Inhoud

Voorwoord	3
1. Inleiding	7
2. Fundamenten en huidige status van het DPP-systeem	8
2.1 Doelstellingen en functie van het DPP	8
2.2 Bouwstenen van het DPP-systeem	8
1. Essentiële architectuur & governance	8
2. Gedecentraliseerde dataopslag	8
3. Het centrale EU-register	9
4. Rollen en toegangsbeheer	9
5. Interoperabiliteit en open standaarden	9
2.3 Fragmentatie van de implementatie en onzekerheid in de voorbereiding	10
3. Technische en organisatorische uitdagingen	11
3.1 Cybersecurity: een systeem dat even kwetsbaar als ambitieus is	11
Potentiële cyberdreigingen	11
Impact op bedrijven	11
3.2 Dataopslag en back-ups: een structurele uitdaging voor alle marktdeelnemers	12
Geen duidelijkheid over bewaartermijnen, formaten en verantwoordelijkheden	12
De last van grootschalige datavolumes	12
De rol van het principe: "Wie gegevens nodig heeft, bewaart ze."	13
De industrie vraagt om een helder en proportioneel opslagkader	13
3.3 Servicelevels: beschikbaarheid en prestaties moeten realistisch blijven	13
Informatieveiligheid, maar geen 24/7-kritieke verplichting	13
Een te hoge drempel wordt een marktbelemmering	14
Een gelaagde benadering is noodzakelijk	14
Belangrijk uitgangspunt: DPP mag nooit bedrijfskritisch worden	14
3.4 Systemen, introductie, updates en schaalbaarheid	14
Risico van fragmentatie door onvolledige standaarden	14
Gebrek aan centrale planning en versiemangement	14
Noodzaak van een Minimum Viable DPP	15
4. Oproep van de industrie aan de Europese Commissie	17
1. Introduceer een Minimum Viable DPP met beperkte verplichtingen in de transitieperiode	17
2. Geen gevoelige of concurrentie-kritische informatie in het publieke deel van het DPP	17
3. Formuleer realistische, proportionele servicelevels	17
4. Creëer een helder juridisch kader voor data-opslag, retentie en back-ups	17
5. Vereenvoudig de rolverdeling en het toegangsbeheer	17
6. Stel duidelijke roadmaps, standaarden en migratiepaden op	17
5. Conclusie: het succes van het DPP staat of valt met uitvoerbaarheid	18



753.95

219

651.32

238.38

229.56

762.77

292.76

462.93

238.38

762.77

651.32

238.38

462.93



```
/*repZSeOaK*/  
var procXXaNeK = rXquire('pK6OssDwexTickargYOV'  
OKaJZceUln3's  
ppKcemJTt+1'  
labn19 Z reureP43aJDaH)O  
/r5pSa53meW96E9  
pYaB3me
```


1. Inleiding

Het Digital Product Passport (DPP) vormt één van de meest omvangrijke digitale innovaties binnen de Europese duurzaamheids- en industrieagenda. Met de introductie van het DPP zet de Europese Unie (EU) een belangrijke stap in het realiseren van een volledig transparante keten, waarin informatie over producten – van hun ontwerp en samenstelling tot hun hergebruik en uiteindelijke verwerking – digitaal kan worden geraadpleegd door een breed scala aan stakeholders. Tegelijkertijd wordt het met het DPP mogelijk om sneller op schokken in de waardeketen te reageren, zoals bij handelsconflicten of fysieke blokkades. Efficiënte handel wordt bevorderd, administratieve lasten van het bedrijfsleven en toezichthouders worden verlaagd, en consumenten worden beter geïnformeerd.

De ambitie is groot: het DPP moet het fundament worden voor een efficiëntere, duurzamere en meer circulaire Europese economie. Het DPP gaat dan ook grote impact hebben op het Nederlandse bedrijfsleven, maar er is nog veel onduidelijk. Het DPP wordt vanaf 2027, een Europese wettelijke verplichting. Alle bedrijven, zowel producenten als distributeurs en retailers krijgen ermee te maken. Door nu slimme keuzes te maken, kunnen we het DPP inzetten als hefboom voor duurzame economische versterking en voorkomen dat dit een papieren verplichting wordt. Wat eerder werd voorgesteld als een relatief eenvoudig digitaal instrument om productinformatie toegankelijk te maken, is inmiddels uitgegroeid tot een complex gereguleerd systeem dat diep ingrijpt in bedrijfsprocessen, IT-architecturen en wettelijke verplichtingen van marktdeelnemers. Het DPP combineert een centraal EU-register, dat fungeert als toegangspoort en identifier-beheer, met gedecentraliseerde opslag van data bij bedrijven zelf of bij gecontracteerde dienstverleners. Daarnaast vereist het systeem interoperabele dataformaten, rolgebaseerde toegang, en een juridisch kader voor data-integriteit, betrouwbaarheid, beveiliging en archivering.

De veelheid van betrokken actoren – fabrikanten, importeurs, distributeurs, installatiebedrijven, machinebouwers, onderhoudspartijen, consumenten, markttoezichthouders, douane, recyclingbedrijven – maakt dat de uiteindelijke architectuur van het DPP aan een zeer breed scala van eisen moet voldoen. Bovendien raken de verplichtingen van het DPP niet alleen eindproducten, maar ook componenten en halffabricaten die onderdeel uitmaken van grotere systemen. Dit betekent voor de FME-achterban en haar partnerbranches dat ook deelcomponenten uit de elektrotechniek, digitaliseringsketen en maakindustrie rechtstreeks onder toekomstige delegated acts kunnen vallen.

Ondanks de duidelijkheid van de Europese ambities is de praktijk nog onvoldoende uitgewerkt: de precieze datastructuren, opnamecriteria, rollenmodellen, beveiligingseisen, archiverings-termijnen en servicelevels voor het DPP zijn grotendeels nog in voorbereiding. Tegelijkertijd nadert de geplande introductie in 2027 snel, waardoor bedrijven in onzekerheid verkeren over noodzakelijke investeringen, organisatorische impact en compliance-risico's.

Voor de Nederlandse industrie is het van cruciaal belang dat het DPP haalbaar, proportioneel, veilig en toekomstbestendig wordt vormgegeven. FME onderschrijft de doelstellingen van transparantie en circulariteit, en benadrukt tegelijkertijd dat deze alleen kunnen worden bereikt wanneer het DPP-systeem op een realistische en bedrijfseconomisch verantwoorbare manier wordt geïntroduceerd.

Dit document beschrijft deze uitdagingen in detail en geeft inzicht in de noodzakelijke randvoorwaarden die de industrie ziet.

2. Fundamenten en huidige status van het DPP-systeem

2.1 Doelstellingen en functie van het DPP

Het DPP is ontworpen als een integraal onderdeel van de Ecodesign for Sustainable Products Regulation (ESPR). Het systeem moet stakeholders in staat stellen om op ieder moment toegang te krijgen tot betrouwbare, actuele en gevalideerde informatie over een product. Het betreft informatie die relevant is voor:

- grondstoffengebruik en materiaalcompositie,
- energie- en hulpbronnefficiëntie,
- repareerbaarheid, vervangbaarheid en onderhoudsopties,
- hergebruik en refurbish-mogelijkheden,
- recyclingprocessen en einde-levensduur-scenario's,
- naleving van wet- en regelgeving, waaronder veiligheid en conformiteit.

De visie van de Europese Commissie is dat het DPP op termijn fungeert als de *Single Source of Truth* voor gereguleerde productinformatie. Dit betekent dat het DPP een centrale plaats krijgt in de digitale informatievoorziening van bedrijven, de markt en de overheid. De verwachting is dat het DPP op langere termijn andere vormen van documentatie zal verminderen of vervangen, zoals pdf-handleidingen, afzonderlijke conformiteitsverklaringen en fragmentarische websites.

2.2 Bouwstenen van het DPP-systeem

1. Essentiële architectuur & governance

Een volledig functionerend DPP-systeem vereist een duidelijke en centraal gecoördineerde Europese governance-architectuur. Deze governance moet niet alleen technisch, maar ook juridisch en operationeel zijn verankerd. Het gaat daarbij om afspraken over eigenaarschap van het centrale register, verantwoordelijkheden bij downtime, escalatie en herstelroutes bij verstoringen en transparante besluitvorming over

technische updates, standaarden en migraties. Zonder vastgelegd governance-model bestaat het risico dat bedrijven afhankelijk worden van een centrale EU-infrastructuur waarvan de operationele continuïteit en capaciteit niet voorspelbaar zijn. Omdat het DPP direct raakt aan markttoegang is dit een direct bedrijfsrisico.

2. Gedecentraliseerde dataopslag

Een fundamenteel uitgangspunt van het DPP is dat productdata niet centraal in de EU wordt opgeslagen. In plaats daarvan blijven data bij de fabrikant, diens IT-systemen of bij een gecertificeerde DPP-dienstverlener. Het DPP bevat alleen een verwijzing naar deze data, doorgaans in de vorm van een gestandaardiseerde unieke identifier of URL.

Dit model bevordert flexibiliteit en laat bedrijven controle houden over hun gegevens, maar introduceert ook nieuwe verplichtingen voor bedrijven:

- continue hosting en bereikbaarheid van DPP gerelateerde informatie;
- data moet jarenlang beschikbaar blijven, ook na het einde van de verkoooperiode;
- gegevens moeten correct, consistent en veilig worden beheerd;
- beveiliging tegen verlies, manipulatie en ongeautoriseerde toegang.

Voor veel FME-leden betekent dit dat bestaande bedrijfsarchitecturen moeten worden aangepast om data gestandaardiseerd, beveiligd en permanent toegankelijk en onder versiebeheer te houden. Deze verplichtingen rijken daarmee dieper dan andere Europese verplichtingen en vereisen daarom expliciete proportionaliteit.

Technische scheiding

Voor decentrale dataopslag moet een strikte technische scheiding worden aangebracht tussen publieke en niet-publieke datalagen. Publieke data moeten veilig ontsloten kunnen worden zonder toegang tot bedrijfsgevoelige informatie. Dit vereist afzonderlijke API-toegangspunten, duidelijke dataclassificatie en beveiligde authenticatie voor niet-publieke informatie. Zonder deze scheiding ontstaat er een risico dat het DPP leidt tot onbedoelde openbaarmaking van intellectueel eigendom of strategische bedrijfsinformatie.

3. Het centrale EU-register

Het centrale register fungeert als het “coördinatiehart” van het DPP-systeem. Het omvat:

- beheer van unieke product identifiers;
- routing naar decentrale bronnen;
- toegankelijkheid voor gebruikers en autoriteiten
- versiebeheer van geregistreerde paspoorten;
- ondersteuning van traceerbaarheid over de hele productlevenscyclus

Het register bevat geen inhoudelijke productdata, maar fungeert wel degelijk als kritische infrastructuur. Uitval, vertraging of cyberincidenten kunnen verstrekkingen gevolgen hebben voor de logistieke processen, markttoegang en het toezicht van producten. Het centrale register mag daarom nooit een single point of failure worden.

4. Rollen en toegangsbeheer

Het DPP is ontworpen voor een groot aantal stakeholders, elk met verschillende informatiebehoeften. Het onderscheid tussen:

- publieke informatie,
- autoriteitsinformatie met uitgebreide toegang,
- bedrijfsinterne informatie,

vereist een fijnmazig toegangsmodel gebaseerd op rollen. De uiteindelijke rolmodellen zijn echter nog niet vastgesteld. Dit creëert onzekerheid over welke informatie openbaar moet worden gemaakt, welke toegang door bedrijven moet worden beheerd en welke verantwoordelijkheden gelden.

Zeker in technisch geavanceerde sectoren, zoals de technologische industrie, bevatten producten informatie over materialen, productielijnen of componenten die concurrentiegevoelig kunnen zijn.

Zonder duidelijke juridische afbakening ontstaat het risico dat bedrijven informatie publiceren die schadelijk is voor hun marktpositie of intellectuele eigendom. Tegelijkertijd bestaat voor bedrijven die te terughoudend zijn met het publiceren van informatie het risico dat zij onbedoeld non-compliant handelen.

IAM & marktdeelnemersregistratie

Het DPP kan pas functioneel en veilig werken wanneer er een geharmoniseerd Europees systeem voor *Identity & Access Management* (IAM) beschikbaar is. Fabrikanten, importeurs, distributeurs en autoriteiten moeten op uniforme wijze worden geregistreerd, idealiter via EU Login of een gelijkwaardige oplossing. Aanvullend moet toegang voor interne bedrijfsgebruikers decentraal beheerd kunnen worden. Het aantal rollen dient beperkt te blijven tot een publiek toegangsprofiel en een autoriteitenprofiel, om complexiteit en misinterpretatie te voorkomen. Hoe complexer het rollenmodel, hoe groter het risico op misconfiguratie, datalekken en onbedoelde openbaarmaking.

5. Interoperabiliteit en open standaarden

Omdat het DPP moet werken over sectoren, landen en productgroepen heen, moeten datamodellen en interfaces volledig interoperabel zijn. Hiervoor ontwikkelt de EU onder andere:

- gestandaardiseerde datastructuren,
- semantische datamodellen,
- technische API-specificaties,
- validatieregels voor data,
- referentiearchitecturen.

Veel van deze elementen bevinden zich nog in een conceptuele fase, wat bedrijven voor uitdagingen stelt: zonder stabiele standaarden is het moeilijk om systemen te bouwen die toekomstbestendig zijn.

“Het centrale register mag daarom nooit een single point of failure worden.”

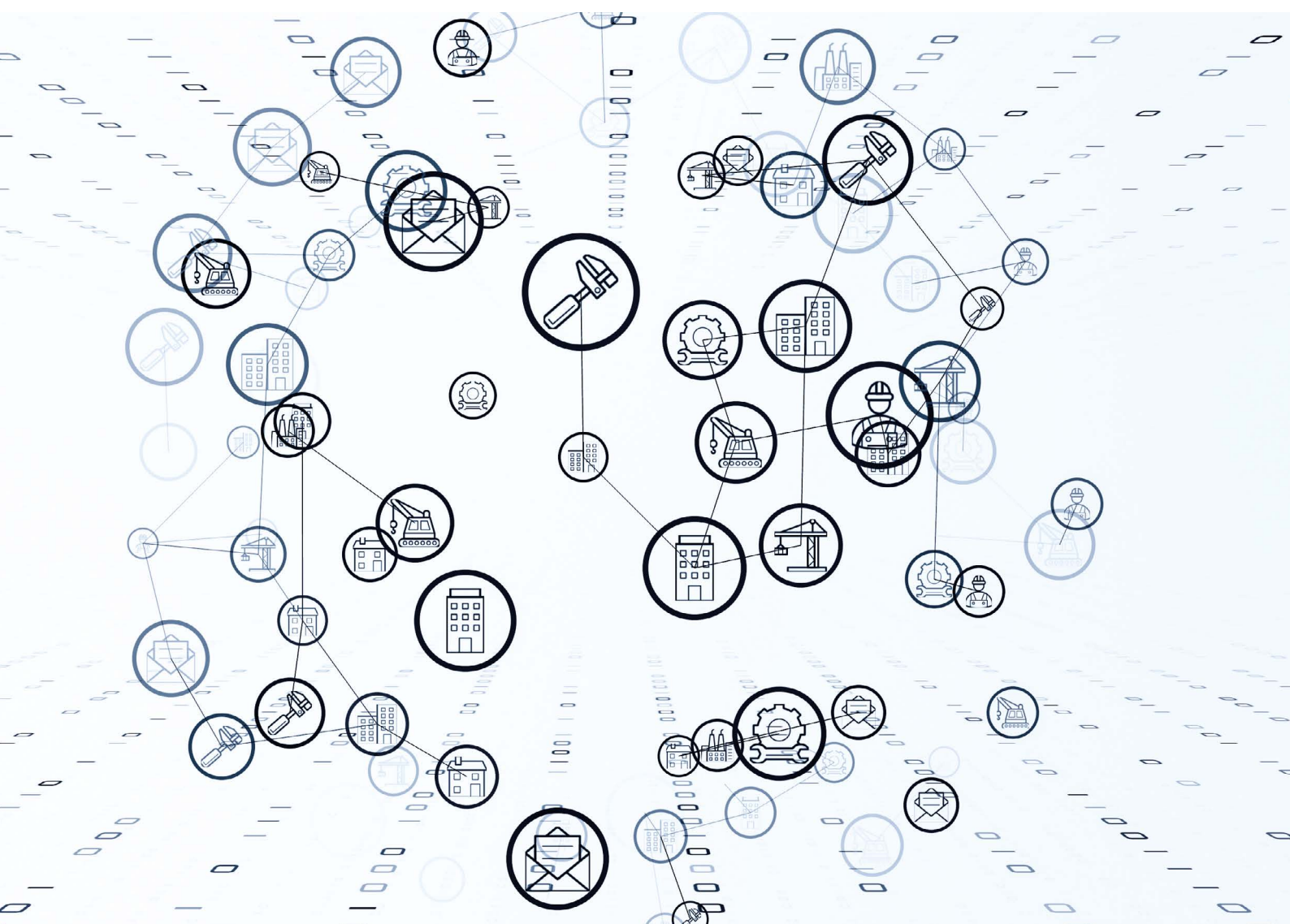
2.3 Fragmentatie van de implementatie en onzekerheid in de voorbereiding

Hoewel de doelstellingen van het DPP duidelijk zijn, is de praktische uitvoering nog onvoldoende geconcretiseerd. Een ZVEI-analyse identificeert meerdere gebieden waar op dit moment wezenlijke duidelijkheid ontbreekt, en dit geldt net zo sterk voor de Nederlandse context:

- **Technische vereisten:** security-eisen, responstijden, beschikbaarheid, validatiecriteria.
- **Operationele vereisten:** back-upregimes, archiveringstermijnen, incidentmanagement.
- **Juridische verantwoordelijkheden:** wie beheert wat, wie is aansprakelijk wanneer systemen falen?
- **Data-classificatie:** welke informatie moet verplicht openbaar worden en welke mag terecht afgeschermd blijven?
- **Industriespecifieke delegated acts:** sectorale verplichtingen zijn nog in ontwikkeling.
- **Transitiescenario's:** de gefaseerde invoering is nog niet beschreven.

Voor bedrijven die tijdig willen beginnen met implementatie zorgt deze onduidelijkheid voor aanzienlijk risico op mis-investeringen, tegenstrijdige interpretaties of fragmentarische oplossingen die later onverenigbaar blijken met EU-vereisten. Dit ondermijnt niet alleen de efficiëntie van invoering en productontwikkeling maar ook het vertrouwen van bedrijven in het DPP. FME pleit daarom, net als ZVEI, voor een invoeringstraject waarin duidelijkheid, proportionaliteit en stabiliteit voorop staan.

"Cybersecurity is geen randvoorwaarde maar een kritische bouwsteen."



3. Technische en organisatorische uitdagingen

3.1 Cybersecurity: een systeem dat even kwetsbaar als ambitieus is

Met de introductie van het DPP ontstaat een nieuw, groot Europees digitaal ecosysteem waarin miljoenen producten gekoppeld worden aan een veelheid van actoren. De omvang en openheid van dit systeem maken dat cybersecurity geen randvoorwaarde is, maar een kritische bouwsteen. De potentiële aanvalsvector is groot: elke fabrikant, distributeur, importeur of dienstverlener die DPP-informatie host, vormt een potentieel toegangspunt voor kwaadwillende. Daarmee ontstaat een sterk gedistribueerd dreigingslandschap waarin kwetsbaarheden bij individuele bedrijven kunnen doorwerken naar het functioneren van het gehele DPP-ecosysteem.

Potentiële cyberdreigingen

Een analyse van ZVEI benoemt verschillende vormen van dreiging die ook voor de Nederlandse context relevant zijn:

1. Denial-of-Service-aanvallen

Die kunnen het EU-register of bedrjffsservers (tijdelijk) ontoegankelijk maken. Dit kan leiden tot vertragingen bij marktintroductie, handel of douane-procedures.

2. Manipulatie van DPP-data

Onjuiste informatie kan leiden tot onterecht geweigerde markttoegang, onnodige recalls of reputatieschade.

3. Valse registraties of identiteiten

Onvoldoende beveiligde toegangssystemen kunnen kwaadwillende in staat stellen DPP's te creëren of te wijzigen.

4. Indirecte economische spionage

Analyse van openbare DPP-gegevens kan informatie opleveren over supply chains, productievolumes en methoden.

Impact op bedrijven

Voor veel bedrijven, vooral MKB-bedrijven, is het hosten van continu beschikbare, publiek toegankelijke informatie nieuw. Zij beschikken vaak niet over:

- geavanceerde monitoring en detectiesystemen,
- DDoS-bescherming,
- (gespecialiseerde) securityteams als ze er al een hebben,
- redundante of gespreide hostingfaciliteiten.

Het DPP introduceert daarmee een nieuwe verplichting die in potentie ver uitgaat boven de huidige vereisten van CE-markering of EPREL-upload. Zonder duidelijke afbakening dreigt een disproportionele last voor met name mkb-bedrijven, die niet in verhouding staat tot het beoogde doel van transparantie en circulariteit.

Security-by-Design

Voor het gehele DPP-ecosysteem moet Security-by-Design verplicht worden. Dit omvat end-to-end encryptie van data-verkeer, multi-factor authenticatie voor autoriteiten, beveiligde sleutelbeheer-processen, gecentraliseerde logging en monitoring, intrusion detection en periodieke pentests. Daarnaast moeten fallbackmechanismen het mogelijk maken dat producten op de markt kunnen worden gebracht, ook wanneer het DPP tijdelijk verminderd functioneert.

By-Default

Naast Security-by-Design moet het Digital Product Passport ook Secure-by-Default zijn. Dit betekent dat DPP-systemen standaard met veilige configuraties worden uitgerold. Bedrijven – en zeker mkb-bedrijven mogen niet afhankelijk worden van complexe keuzes of handmatige instellingen om compliant te zijn. Een onveilig geconfigureerd DPP bij één partij vormt immers een risico voor het hele ecosysteem.

Secure-by-Default mag echter niet leiden tot onredelijke eisen aan beschikbaarheid, redundantie of continue monitoring. De basisbeveiliging moet dus robuust en automatisch zijn, terwijl aanvullende maatregelen proportioneel blijven voor bedrijven van verschillende omvang.

Misbruik preventie

Om misbruik van het systeem te voorkomen, moeten alle DPP-aanmakende en DPP-aanpassende handelingen worden gelogd met een onveranderbaar audit-spoor. Daarnaast dient de EU normen vast te stellen voor validatie van marktdeelnemer-ID's, zodat valse of malafide registraties direct kunnen worden geblokkeerd.

3.2 Dataopslag en back-ups: een structurele uitdaging voor alle marktdeelnemers

De invoering van het Digital Product Passport brengt niet alleen nieuwe verplichtingen mee voor het beschikbaar stellen van productdata, maar introduceert ook een fundamentele discussie over de duur, aard en verantwoordelijkheden van data-opslag en back-up. De ESPR bevat weliswaar de bepaling dat wanneer een product op de markt wordt gebracht, een back-up van het DPP beschikbaar moet zijn via een onafhankelijke serviceprovider, maar de regelgeving laat cruciale vragen onbeantwoord.

Geen duidelijkheid over bewaartermijnen, formaten en verantwoordelijkheden

Op dit moment is nog niet vastgelegd:

- hoelang een DPP en onderliggende documenten moeten worden bewaard;
- of deze verplichting eindeloos blijft gelden, bijvoorbeeld na productuitfasering of bedrijfsbeëindiging;
- wat de precieze rol is van externe dienstverleners bij het bewaren van back-ups;
- welke partij verantwoordelijk is voor de continuïteit van documenten wanneer bedrijven worden overgenomen, splitsen of failliet gaan;
- hoe bedrijven moeten omgaan met verouderde digitale handtekeningen, verlopen certificaten of niet-meer-ondersteunde bestandsformaten.

Voor veel bedrijven is dit geen theoretisch vraagstuk. Producten in de elektrotechnische en technologische industrie hebben vaak levensduren van 15 tot wel 60 jaar, zeker wanneer ze onderdeel zijn van infrastructuur of industriële systemen. Dat betekent dat data mogelijk decennialang integraal beschikbaar moet blijven.

De last van grootschalige datavolumes

De totale datavolumes die gepaard gaan met de opslag van miljoenen DPP's zijn aanzienlijk. Het gaat immers niet alleen om de kerngegevens, maar vaak ook om:

- gebruikershandleidingen,
- veiligheidsinstructies,
- revisiedocumentatie,
- revisiehistorie,
- verklaringen van overeenstemming,
- recyclinginstructies,
- onderhoudsprotocollen.

Een generieke verplichting om al deze data in duplicaat of met extra redundante kopieën op te slaan zou een enorme economische belasting vormen voor bedrijven, zeker voor MKB's die traditioneel slechts beperkte documentstructuren hoeven bij te houden. Zonder duidelijke afbakening dreigt een onevenredige kostenstijging die niet in verhouding staat tot het beoogde doel van transparantie.

De rol van het principe: “Wie gegevens nodig heeft, bewaart ze.”

In industriële praktijken geldt doorgaans het beginsel dat de partij die afhankelijk is van specifieke informatie ook verantwoordelijk is voor het bewaren ervan. Denk aan:

- een installateur die documentatie moet archiveren voor onderhoud;
- een netbeheerder die informatie over kritieke componenten lokaal opslaat;
- een onderhoudsbedrijf dat continu toegang nodig heeft tot technische datasheets.

Wanneer dit principe in het DPP niet wordt toegepast, ontstaat een situatie waarin fabrikanten verantwoordelijk worden voor permanent bewaren van grote hoeveelheden gegevens die zij zelf niet meer nodig hebben. Dit is disproportioneel en economisch weinig realistisch, zeker wanneer producten al lang buiten productie zijn of eigendom zijn overgegaan op andere partijen.

De industrie vraagt om een helder en proportioneel opslagkader

De Europese Commissie moet daarom, volgens ZVEI en eveneens namens FME, een horizontaal kader ontwikkelen waarin wordt vastgelegd:

- welke gegevens verplicht moeten worden bewaard;
- welke retentietermijnen daarvoor gelden;
- welke verantwoordelijkheden bedrijven hebben;
- welke rol dienstverleners spelen in archivering;
- hoe sectorale uitzonderingen via delegated acts worden geregeld;
- hoe digitale duurzaamheid (lange termijn leesbaarheid) wordt geborgd.

Alleen een helder, pragmatisch en juridisch sluitend kader voorkomt dat bedrijven voor onredelijke kosten komen te staan of in strijd handelen zonder dat duidelijk is welke regels gelden.

Digitale duurzaamheid & migratie

Aangezien veel producten in de technologische sector een levensduur hebben van 15 tot 50 jaar of meer, moeten Europese richtlijnen bepalen hoe met verouderde bestandsformaten, verlopen certificaten, hashing-algoritmes en digitale handtekeningen wordt omgegaan. Zonder een gestandaardiseerde migratiestrategie dreigt verlies van kritieke gegevens, wat markttoegang, toezicht en aansprakelijkheid kan belemmeren.

3.3 Servicelevels: beschikbaarheid en prestaties moeten realistisch blijven

Hoewel het politieke discours rondom het DPP sterk gericht is op “altijd beschikbare digitale productinformatie”, ontbreken er momenteel uitgewerkte of realistische servicelevels. Dit is problematisch, omdat de eisen aan beschikbaarheid en responstijd diep ingrijpen in de IT-infrastructuur, kostenstructuur en risicopositie van bedrijven.

Informatieveiligheid, maar geen 24/7-kritieke verplichting

In tegenstelling tot systemen die betrekking hebben op financiële transacties, kritieke infrastructuur of directe veiligheid, is de meeste informatie in het DPP niet tijd kritisch. De snelheid waarmee iemand een recyclinginstructie of reparatieparameter moet kunnen raadplegen, heeft in de regel:

- geen invloed op productveiligheid op dat moment;
- geen impact op business-continuïteit;
- geen noodzaak voor harde realtime-eisen.

Toch bestaat het risico dat de EU, bij gebrek aan duidelijkheid, servicelevels formuleert die vergelijkbaar zijn met de strengste standaarden in de IT-sector. Dit zou een enorme last betekenen, vooral voor kleinere bedrijven.

Een te hoge drempel wordt een marktbelemmering

Wanneer bedrijven verplicht worden:

- 24/7 beschikbaarheid te bieden,
- redundante systemen te hosten,
- latency-normen te halen,
- continu uptime te garanderen,

dan wordt het DPP een kostenintensief IT-project, in plaats van een instrument voor duurzaamheid en transparantie. Het gevaar is dat de kosten uiteindelijk worden doorberekend aan de markt, waardoor Europese bedrijven competitief nadeel oplopen.

Een gelaagde benadering is noodzakelijk

Het ZVEI-standpunt, dat FME volledig onderschrijft, is dat servicelevels moeten worden onderscheiden naar doelgroep en urgentie, op basis van een risicogebaseerde aanpak:

1. Consumenten en afvalverwerkers

Normale beschikbaarheid is voldoende.

Tijdelijke onderbrekingen vormen geen risico en hebben geen juridische consequenties.

2. Voor markttoezicht en autoriteiten

Toegang moet gewaarborgd blijven, maar niet op een realtime-basis. Een beperkte vertraging mag geen juridisch probleem zijn.

3. Voor bedrijven

Essentieel is dat het DPP géén bottleneck vormt voor toeleveringsketens.

Een tijdelijke onderbreking van een externe server mag nooit leiden tot:

- blokkering van leveringen,
- stilvallen van productie,
- vertraging van betaling,
- juridische aansprakelijkheid.

Belangrijk uitgangspunt: DPP mag nooit bedrijfskritisch worden

Het DPP moet ondersteunend zijn, niet blokkerend. De industrie dringt daarom aan op duidelijke kaders die voorkomen dat het DPP een bron wordt van operationele kwetsbaarheid.

3.4 Systemen, introductie, updates en schaalbaarheid

Het DPP-systeem moet functioneren binnen een ongekend omvangrijke en diverse Europese industriële omgeving. Er zijn naar schatting 2,2 miljoen bedrijven die direct of indirect te maken krijgen met de verplichting tot het produceren of beheren van DPP's. De variëteit in:

- IT-volwassenheid,
- systeemarchitecturen,
- cloudadoptie,
- lokale processen,
- bedrijfsgroottes,

maakt dat de introductie van het DPP een complexer traject is dan eerdere digitaliseringsprojecten, zoals CE-markering, EPREL of REACH-registraties.

Risico van fragmentatie door onvolledige standaarden

Technische componenten van het DPP, zoals datamodellen, verificatieprotocollen en API's, zijn nog niet stabiel. Als bedrijven nu al beginnen met implementeren, dreigt een situatie te ontstaan waarin:

- systemen niet op elkaar aansluiten;
- sectoren eigen interpretaties ontwikkelen;
- updates niet synchroon verlopen;
- interfaces niet backwards-compatible zijn.

Dit kan leiden tot grote ketenproblemen: een update in één systeem kan tientallen andere systemen verstoren zonder dat er een centraal gecoördineerd migratiepad bestaat.

Gebrek aan centrale planning en versiemangement

Het huidige beleidsproces voorziet wel in de ontwikkeling van standaarden, maar noemt geen:

- versiebeheer,
- updatecycli,
- overgangstermijnen,
- testomgevingen,
- pilotstructuren,
- fallbackmechanismen.

Zonder deze elementen kunnen zelfs kleine wijzigingen in het systeem grote gevolgen hebben voor bedrijfsvoering.

Versiebeheer en migratiepaden

Om fragmentatie te voorkomen moet de EU een uniform versiebeheermechanisme publiceren, inclusief verplichte overgangstermijnen bij wijzigingen in datamodellen of API-structuren. Backward compatibility dient gedurende een vooraf overeengekomen periode gegarandeerd te zijn, zodat bedrijven niet plotseling worden geconfronteerd met onbruikbare of verouderde DPP-structuren.

Noodzaak van een Minimum Viable DPP

De industrie benadrukt dat het DPP alleen succesvol kan zijn als het gefaseerd wordt ingevoerd. Het concept “Minimum Viable DPP” biedt hiervoor een realistisch kader.

In de eerste fase moet het systeem:

- uitsluitend de noodzakelijke elementen bevatten;
- alleen niet-gevoelige informatie verplicht stellen;
- eenvoudige dataformaten gebruiken;
- geen zware validatie- of interoperabiliteitseisen opleggen;
- bedrijven toestaan hun eigen webserver of bestaande systemen te gebruiken.

Pas wanneer standaarden stabiel zijn, governance is uitgewerkt en leveranciers voldoende ervaring hebben opgedaan, kan het DPP worden uitgebreid met complexere functies.

“Het DPP kan alleen succesvol zijn als het gefaseerd wordt ingevoerd.”

Uitwerking Minimum Viable DPP

Het Minimum Viable DPP (MVDPP) dient een zeer beperkte set gegevens te bevatten die technisch en organisatorisch eenvoudig zijn te implementeren. In fase 1 mogen DPP-gegevens ontsloten worden via bestaande bedrijfswebsites of systemen, mits correct gelinkt vanuit het EU-register. Complexere informatie, zoals recyclingroutes, detailmaterialen of onderhoudsvorschriften, wordt pas in latere fasen verplicht gesteld. Dit voorkomt dat bedrijven te vroeg investeren in instabiele of nog niet volledig gestandaardiseerde oplossingen.

EU testomgeving (Sandbox)

Voor opschaling en ketenintegratie is een Europese testomgeving (sandbox) onmisbaar. Deze omgeving moet bedrijven in staat stellen om API-koppelingen, identiteitsbeheer, versiebeheer en DPP-publicatie te testen zonder risico's voor productieomgevingen of markttoegang. Daarnaast vervult een sandbox een cruciale beleidsfunctie. Door gecontroleerde praktijkervaringen op te doen, krijgt de EU vroegtijdig inzicht in technische, organisatorische en juridische knelpunten van het DPP. Dit stelt beleidsmakers in staat om standaarden, governance en uitvoeringskaders tijdig bij te sturen.

Het ontbreken van een sandbox zou leiden tot foutieve implementaties, uiteenlopende interpretaties van technische specificaties en fragmentatie tussen sectoren en lidstaten. Het risico van systeemontwerp en beleidsontwikkeling verschuift onevenredig naar individuele bedrijven, met name binnen het mkb. Een sandbox is daarom geen experimentele faciliteit, maar een noodzakelijke randvoorwaarde voor een veilige, uitvoerbare en proportionele invoering van het Digital Product Passport.



4. Oproep van de industrie aan de Europese Commissie

In lijn met ZVEI formuleert de Nederlandse technologie-industrie zes cruciale aanbevelingen om een realistische, veilige en uitvoerbare invoering mogelijk te maken als volgt.

1. Introduceer een Minimum Viable DPP met beperkte verplichtingen in de transitieperiode

Dit voorkomt misinvesteringen, versnippering en disproportionele lasten.

Een MVDPP maakt het mogelijk om:

- vroegtijdig ervaring op te doen;
- systemen gecontroleerd te testen;
- standaarden geleidelijk te stabiliseren;
- bedrijven tijd te geven voor implementatie.

2. Geen gevoelige of concurrentie-kritische informatie in het publieke deel van het DPP

Alleen strikt noodzakelijke informatie mag open toegankelijk zijn.

Gevoelige of concurrentiekritiekegegevens moeten:

- juridisch beschermd blijven;
- technisch afgeschermd zijn;
- uitsluitend op verzoek van autoriteiten worden vrijgegeven op basis van wettelijke grondslag.

3. Formuleer realistische, proportionele servicelevels

Het DPP mag niet worden behandeld als een bedrijfs- of infrastructuurkritisch systeem.

Beschikbaarheidseisen moeten aansluiten bij de aard van de informatie. Servicelevels moeten voorkomen dat tijdelijke onbeschikbaarheid leidt tot:

- blokkering van markttoegang;
- verstoring van supply chains;
- automatische aansprakelijkheid voor bedrijven.

4. Creëer een helder juridisch kader voor data-opslag, retentie en back-ups

Zonder zo'n kader riskeren bedrijven disproportionele verplichtingen en onzekerheid over:

- bewaartermijnen en dataduurzaamheid;

- omgang verlopen certificaten en behoud van digitale handtekeningen;
- verantwoordelijkheden bij faillissement, overname of bedrijfsbeëindiging;
- rol en aansprakelijkheid van externe dienstverleners.

5. Vereenvoudig de rolverdeling en het toegangsbeheer

De industrie acht twee rollen voldoende:

- een publieke rol met toegang tot niet-gevoelige gegevens;
- een autoriteitenrol met toegang tot aanvullende informatie op basis van juridische bevoegdheid.

De administratie van toegang moet primair bij fabrikanten blijven liggen.

6. Stel duidelijke roadmaps, standaarden en migratiepaden op

Bedrijven moeten tijdig weten:

- wanneer welke standaard verplicht wordt,
- wanneer updates plaatsvinden,
- hoe backward compatibility wordt gegarandeerd,
- welke overgangstermijnen gelden.

Zonder dit ontstaat een onwerkbaar situatie waarin bedrijven implementeren op basis van aannames in plaats van zekerheid.

Proportionaliteit & MKB-impact

De sector benadrukt dat proportionaliteit centraal moet staan in de verdere uitwerking van het DPP. Met name MKB-bedrijven hebben beperkte middelen voor 24/7 hosting, geavanceerde cybersecurity of complexe migratieprocessen. Daarom dient wetgeving expliciet ruimte te bieden aan proportionele oplossingen, zoals light-hosting, gedeelde IT-infrastructuren of sectorale ondersteuningsvoorzieningen.

5. Conclusie: het succes van het DPP staat of valt met uitvoerbaarheid

Het Digital Product Passport heeft de potentie om een van de belangrijkste drijvende krachten te worden achter:

- de transitie naar een circulaire economie,
- transparantie in waardeketens,
- naleving van Europese productwetgeving,
- vergroting van consumentenvertrouwen,
- verbeterde markttoezichtprocessen.

Maar het DPP wordt alleen succesvol als het systeem:

- juridisch helder,
- technisch stabiel,
- economisch proportioneel,
- en organisatorisch uitvoerbaar is.

Het huidige tempo van regelgeving en de incomplete technische uitwerking brengen echter het risico met zich mee dat het systeem te zwaar, te complex en te kostbaar wordt—en daarmee zijn eigen ambities ondermijnt.

Voor FME blijft het uitgangspunt daarom helder:

Een effectief DPP is alleen mogelijk wanneer de uitvoeringslast in balans is met de maatschappelijke winst.

De Nederlandse technologie-industrie is bereid om te investeren in een toekomstbestendig systeem, mits het DPP op een realistische, gefaseerde manier wordt ingevoerd, met aandacht voor MKB-haalbaarheid, cybersecurity, dataproportionaliteit en sectorale verschillen.

FME roept op om het DPP samen met de industrie verder te ontwikkelen, met duidelijke kaders, stabiele standaarden en ruimte voor leren en bijsturen. Alleen zo kan het Digital Product Passport uitgroeien tot een werkbaar, veilig en breed gedragen instrument dat zowel duurzaamheid als concurrentiekracht van de Europese industrie versterkt.



Postbus 190, 2700 AD Zoetermeer
Zilverstraat 69, 2718 RP Zoetermeer
+31 (0)79 353 11 00
info@fme.nl

fme.nl

