

ESPR Digital Product Passport: Wat betekend dit voor de industrie?

Paul Borghouts en Marlou Snelders | FEDET Juni 2026

De Europese belofte van het Digitaal Product Paspoort



Circulariteit

Beter inzicht in materialen, hergebruik, reparatie en end-of-life van producten



Transparantie

Meer zicht op productinformatie in de keten en betere informatie voor ketenpartners



Compliance

Eén structuur voor productinformatie, conformiteit, relevante productvereisten en efficiënter markttoezicht



Efficiëntie

Minder dubbel werk en soepelere informatie-uitwisseling in de keten

Op papier belooft het DPP meer circulariteit, transparantie, compliance en efficiëntie.

De werkelijkheid voor de industrie

Nog veel open

Standaarden, governance en productscope zijn nog in beweging.

Uitvoerbaarheid telt

Implementatie vraagt data, systemen, capaciteit en duidelijke proportionaliteit.

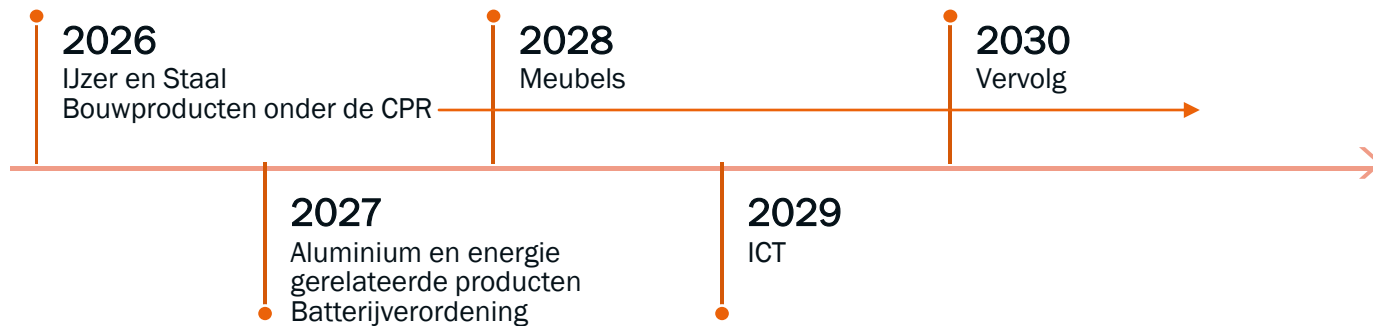
Gevoelige vragen

Toegang tot data, rollen in de keten en aansprakelijkheid zijn nog niet uitgekristalliseerd.

Scope: wie krijgt ermee te maken?

Fabrikanten · Importeurs · Distributeurs · Installatiebedrijven · Machinebouwers · Recyclingbedrijven · Autoriteiten & douane

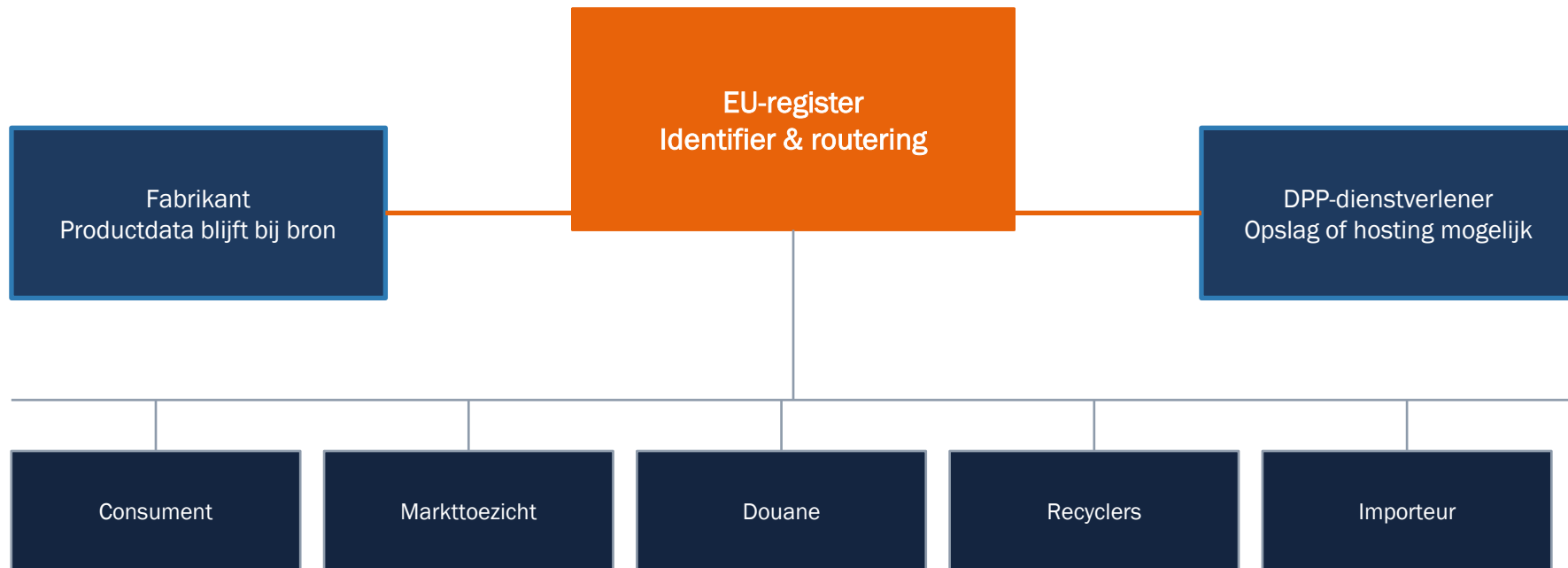
Tijdlijn & Scope



De DPP-verplichting wordt productgroep voor productgroep ingevoerd via gedelegeerde handelingen.

Voor FME-leden betekent dit: nu al voorbereiden op productdata, governance en ketensamenwerking, terwijl scope, datapunten en exacte termijnen per delegated act nog verder worden uitgewerkt.

DPP: centraal ontsloten, decentraal opgeslagen



Wat kunnen bedrijven nog niet vastleggen?

⚠ De uitrol komt dichterbij, terwijl cruciale uitvoeringskeuzes nog openstaan.

Technische vereisten

Beveiliging, beschikbaarheid, validatie en responstijden zijn nog niet eenduidig uitgewerkt.

Operationele vereisten

Back-up, archivering en incidentafhandeling zijn nog niet uniform vastgelegd.

Juridische aansprakelijkheid

Rolverdeling en aansprakelijkheid bij fouten of storingen zijn nog niet scherp afgebakend.

Data-classificatie

De grens tussen verplichte openbaarheid en afgeschermd bedrijfsinformatie is nog niet helder.

Delegated acts

Productspecifieke verplichtingen en detailniveau volgen pas in sectorspecifieke uitwerking.

Implementatiepad

Fasering, overgangstermijnen en het praktische invoeringspad zijn nog niet concreet beschreven.

Cybersecurity bepaalt de betrouwbaarheid van DPP-ecosysteem



DoS-aanvallen

Uitval van register of bedrijfsomgeving kan leiden tot vertraging bij markttoegang, controles en uitlevering.



Datamanipulatie

Onjuiste of gewijzigde DPP-data kan leiden tot recalls, afkeur en reputatieschade.



Valse registraties en misbruik

Zwakke beveiliging vergroot het risico op ongeautoriseerde aanmaak, wijziging of misbruik van paspoorten.



Economische spionage

Analyse van toegankelijke DPP-data kan concurrentiegevoelige inzichten geven in ketens, volumes en herkomst.

Security-by-design en secure-by-default moeten uitgangspunt zijn voor het volledige DPP-ecosysteem.

Wat betekent dit voor uw bedrijf?

Nu al doen

- Bepaal welke producten/materialen (waarschijnlijk) in scope komen
- Breng productdata en eigenaarschap in kaart
- Breng IT-landschap in kaart
- Volg sectorspecifieke delegated acts
- Deel knelpunten en praktijkinput via FME

Nog geen definitieve keuzes maken

- Definitieve datamodellen en API-specificaties
- Sectorspecifieke bewaartermijnen
- Definitieve IAM-oplossing en toegangsmodel (EU login)
- Concrete servicelevels en beschikbaarheidseisen

Risico's bewaken

- Mis-investeringen in nog instabiele standaarden
- Concurrentiegevoelige informatie in publieke DPP-data
- Disproportionele hosting- en beheerplichten voor het MKB
- Juridische aansprakelijkheid bij uitval of fouten in het systeem

Opslag, bewaartermijnen en continuïteit zijn nog niet helder

Waar de knelpunten nu zitten

- Geen heldere bewaartermijnen
- Onzekerheid bij overname of faillissement
- Verouderende formats, handtekeningen en certificaten
- Zeer grote datavolumes en documentatie

Digitale fragmentatie ondermijnt werkbaarheid

2-3 mln

bedrijven in directe potentiële scope
maar
relevant voor bedrijven in de gehele keten

Waar fragmentatie bedrijven raakt

- Standaarden blijven in beweging
- Sectoren kiezen eigen interpretaties
- Updates lopen niet gelijk op
- Koppelingen verouderen snel

Werkbare route: begin klein

Fase 1: start met de noodzakelijke kerngegevens, eenvoudige formats en bestaande systemen

Fase 2: breid pas uit zodra standaarden stabiel zijn en governance is uitgewerkt

6 aanbevelingen voor een werkbaar DPP

1

Minimum Viable DPP

Beperk verplichtingen in de transitieperiode en voer sectorspecifiek gefaseerd in

2

Geen gevoelige data openbaar

Bescherm intellectueel eigendom juridisch en technisch; alleen delen met bevoegde autoriteiten

3

Proportionele servicelevels

Laat eisen aansluiten op het type informatie en voorkom automatische aansprakelijkheid bij uitval

4

Helder opslagkader

Leg retentie, digitale duurzaamheid en verantwoordelijkheid vast bij uitval, fusie of faillissement

5

Eenvoudig toegangsbeheer

Werk met een publiek profiel en een autoriteitenprofiel, met beheer bij de fabrikant

6

Duidelijke roadmaps

Leg standaarden, updatecycli, backward compatibility en overgangstermijnen tijdig vast

Conclusie

Het DPP kan een belangrijke versneller worden van de transitie naar een circulaire Europese economie — mits de uitwerking aansluit op de praktijk van bedrijven.



Juridisch werkbaar



Technisch robuust



Economisch haalbaar

**FME roept op: ontwikkel het DPP samen met de industrie.
Heldere kaders · stabiele standaarden · ruimte om te leren en bij te sturen.**