Over FME

FME is de ondernemersorganisatie voor de technologische industrie. Onze 2.100 leden zijn technostarters, handelsbedrijven, middelgrote en kleine industrie en grote industrie/multinationals die actief zijn in de sectoren metaal, elektronica, elektrotechniek en kunststof. Er werken bij onze leden 220.000 medewerkers. De gezamenlijke omzet van de FME-leden bedraagt € 139 miljard, waarvan € 59 miljard afkomstig is uit export. Dit benadrukt de cruciale rol van de technologische industrie binnen onze economie: deze sector genereert direct 12% van het nationale inkomen, en wanneer ook de indirecte effecten worden meegenomen, stijgt dit aandeel tot 20%.

FME Beleidsaanbevelingen Digitale Omnibus

De recente golf van EU-wetgeving op het gebied van digitalisering, zoals de AI Act, Data Act, CRA en NIS2, heeft geleid tot een toename van fragmentatie in regelgeving en complexiteit voor bedrijven in de (high tech) maakindustrie. Dit heeft grote gevolgen voor de sector, terwijl juist deze bedrijven een sleutelrol vervullen in het realiseren van de groene en digitale transitie van Europa.

In plaats van duidelijkheid en rechtszekerheid te bieden, leidt de snelle opeenvolging van EU-wetgeving tot een steeds meer gefragmenteerde, belastende en inconsistente regelgevingsomgeving, met hoge administratieve kosten. Deze uitdagingen zijn bijzonder groot voor mkb'ers en systeemleveranciers die in meerdere sectoren en waardeketens actief zijn. Volgens onderzoek in de sector heeft 70 % van de bedrijven al innovatieprojecten stopgezet vanwege bezorgdheid over de regelgeving. Dit ondermijnt het vermogen van de Europese industrie om te innoveren, op te schalen en veerkrachtig te opereren in een geopolitiek context, waarin juist dat een topprioriteit zou moeten zijn.

FME verwelkomt de ambitie van de Europese Commissie om via het Digital Omnibuspakket digitale wetgeving te vereenvoudigen, te harmoniseren en daarmee de administratieve lasten met 25 % in het algemeen en 35 % voor het mkb te verminderen. Dit pakket biedt een broodnodige kans om te komen tot een écht coherent en op de uitvoering gericht kader, dat rekening houdt met het mkb en het concurrentievermogen van Europa versterkt. Om dit te garanderen en de strategische autonomie van Europa te versterken, doen wij vijf aanbevelingen:

1. Duidelijke definities en terminologie

Belangrijke termen zoals 'product met digitale elementen', 'AI-systeem', 'veiligheidscomponent' of 'technische documentatie' worden momenteel in verschillende wetten verschillend gedefinieerd, wat tot verwarring en rechtsonzekerheid leidt.

Zo wordt een fabrikant van robotica geconfronteerd met uiteenlopende definities van “AI-systeem” in de Verordening AI (AI Act) (2024/1689), en de Machineverordening (2023/1230). Dit leidt tot twee afzonderlijke conformiteitsprocedures voor hetzelfde product, met uiteenlopende documentatie eisen ondanks dat de functionaliteit niet is veranderd. De verschillende definities van ‘veiligheidscomponent’ tussen de AI-Act en de Machineverordening illustreren dit probleem. Daarnaast komen termen als ‘*dark patterns*’ inconsistent voor in de Digital Services Act (DSA) (2022/2065), Digital Markets Act (DMA) (2022/1925) en Data Act (2023/2854).

Daarnaast ontstaan knelpunten waar verschillende wetgevingskaders elkaar raken. De Data Act, spreekt bijvoorbeeld over ‘gebruiker’ en ‘datahouder’, terwijl de GDPR uitgaat van ‘datasubject’ en ‘verwerkingsverantwoordelijke’. Dit leidt tot conflicten wanneer de gebruiker van een slim apparaat niet dezelfde persoon is als het datasubject wiens gegevens verwerkt worden, terwijl de fabrikant formeel de datahouder is.

FME pleit voor het volgende:

- Stel een levende centrale woordenlijst op onder de Omnibus, geïntegreerd in richtsnoeren en uitvoeringsbesluiten om juridische consistentie te waarborgen.
- Heldere afbakening van rollen in de GDPR en Data Act: wie heeft welke rechten en plichten als gebruiker, datasubject en datahouder niet samenvallen?
- Verwijder doublures en tegenstrijdige interpretaties in parallelle wetten

2. Stroomlijn rapportageverplichtingen

Bedrijven moeten hetzelfde beveiligingsincident meerdere keren rapporteren: aan nationale CSIRT's onder NIS 2 Directive (NIS2) (2022/2555), aan ENISA onder de CRA en soms ook aan andere autoriteiten onder sectorale wetgeving. Dit staat haaks op het door de Commissie geformuleerde doel om multifunctionele rapportage te faciliteren en dubbel werk in de cyberbeveiligingswetgeving te voorkomen.

Bovendien begint deze versnippering al eerder in het proces, namelijk bij de registratie. Voor veel bedrijven is het onduidelijk welke rechtspersoon binnen een bedrijfsgroep onder NIS2 moet worden geregistreerd en in welk land. In tegenstelling tot de General Data Protection Regulation (GDPR) (2026/697), definieert NIS2 geen concept van ‘*group company*’ dat als leidraad zou kunnen dienen voor de aanwijzing van een centrale entiteit. Als gevolg daarvan worden bedrijven geconfronteerd met aanzienlijke rechtsonzekerheid.

FME pleit voor het volgende:

- Ontwikkel één Europese registratiestructuur (ten minste voor NIS2)
- De rapportageverplichtingen op het gebied van cyberbeveiliging in NIS2, CRA en sectorale wetgeving op elkaar afstemmen en stroomlijnen.

- Ontwikkel één Europees meldingsmechanisme voor cyberincidenten, in nauwe samenwerking met ENISA en nationale CSIRT's, zoals voorzien in de CRA. Stel dit mechanisme open voor NIS2-meldingen, om onduidelijkheid en fouten te voorkomen, bijvoorbeeld complexe bedrijfsmodellen.

3. Harmoniseer horizontale en sectorale vereisten

Horizontale wetgeving (AI-Act, GDPR, CRA) kent veel overlap met sectorspecifieke productwetgeving (Machineverordening en Medische Hulpmiddelenverordening). Dit leidt tot dubbele conformiteitsbeoordelingen en vergroot de rechtsonzekerheid. Bedrijven weten niet welke zeker welke regels voorrang hebben of welke beoordeling volstaat. Daarnaast kunnen toezichthouders de regels anders interpreteren, waardoor een product mogelijk in één land wel kan worden goedgekeurd en in het andere wordt tegengehouden. Dit kan dus niet alleen zorgen voor een gebrek aan rechtszekerheid maar ook voor een ongelijk speelveld.

FME pleit voor het volgende:

- Zorg ervoor dat bedrijven via één traject kunnen aantonen dat hun product voldoet en dubbele high-risk verplichtingen worden voorkomen. Integreer vereisten alleen in sectorale kaders wanneer dit relevant en evenredig is.
- Stem de Data Governance Act (DGA) Art. 12 af op het Digitale Product Paspoort (DPP), zodat overlappende registratie- en governance-eisen worden vermeden. Zorg ervoor dat een DPP-provider niet automatisch ook een '*data-intermediary'* is, tenzij dit expliciet relevant is.
- Verduidelijk “lex specialis”-relaties en voorkom dat horizontale regels sectorspecifieke kaders dubbel of tegenstrijdig aanvullen.

4. Realistische implementatie en transitietermijnen

Veel nalevingsverplichtingen in de CRA en AI-Act zijn afhankelijk van geharmoniseerde technische normen, die nog in ontwikkeling zijn. De invoering van nieuwe verplichtingen vraagt aanzienlijke voorbereidingstijd: voor het ontwikkelen van normen, het aanpassen van producten en processen, het trainen van personeel en het afstemmen met toeleveranciers. Volgens de huidige planning zullen de belangrijkste normen vanwege de complexiteit van het consensusvormingsproces niet vóór december 2026 beschikbaar zijn. Niet alleen het bedrijfsleven, maar ook aangemelde instanties en markttoezichtautoriteiten hebben voldoende voorbereidingstijd nodig.

FME pleit voor het volgende:

- Zorg voor haalbare termijnen die aansluiten bij de beschikbaarheid van standaarden.
- Verleng waar nodig de overgangsperiodes voor belangrijke wetten zoals de CRA en de AI-Act: stel de toepassing van *high-risk requirements* uit tot 12 maanden na publicatie van geharmoniseerde normen. Geef fabrikanten ten minste 12 maanden om de

verticale normen bij de CRA na officiële publicatie te implementeren in hun ontwikkelings- en productieprocessen en sta Module A (*internal production control)* toe als conformiteitsbeoordelingsprocedure voor 'belangrijke producten'(Annex III, Class I) totdat *vertical standards* beschikbaar zijn.

- Schort sancties op totdat naleving technisch haalbaar is en *harmonised standards* en *guidelines* zijn vastgesteld.

5. Zorg voor evenredigheid van B2B-toepassingen en mkb-fabrikanten

B2B-industriële systemen (bijv. fabrieksrobots, sensoren, elektriciteitsnetapparatuur) hebben heel andere risicoprofielen dan consumentenproducten. Lange productlevenscycli, complexe integratie met verouderde systemen en contractuele risicospreiding komen veel voor in industriële omgevingen.

FME pleit voor het volgende:

- Sta vereenvoudigde technische documentatie en ondersteuningsverplichtingen toe voor industriële componenten met lange innovatiecycli.
- Maak een uitzondering in de CRA voor eenvoudige producten met digitale elementen die redelijkerwijs en technisch geen cyberrisico kunnen vormen (*benign products*) zoals in de EMC (2014/30/EU).
- Maak onderscheid in de digitale levensduur van fysieke levensduur, zodat updates niet decennia verplicht blijven.
- Breid de vereenvoudigingsbepalingen van artikel 33 CRA (mkb-clausule) uit naar alle laag risicoproducten, ongeacht de grote van de fabrikant.

Van beleid naar praktijk: de noodzaak van een op de industrie gebaseerde implementatie

FME staat volledig achter de verschuiving van de focus van de Europese Commissie van wetgeving naar implementatieresultaten. Om succesvol te zijn, moet de Omnibus leiden tot een regelgevingskader dat coherent is over verschillende wetten heen, voorspelbaar in toepassing en werkbaar in de industriële realiteit van complexe waardeketens.

We roepen de Nederlandse regering op om deze prioriteiten actief in Brussel te promoten en samen te werken met lidstaten én belanghebbenden bij het vormgeven van de nationale implementatie, zodat nationale koppen worden voorkomen en een gelijk speelveld te waarborgen.

In een tijd van wereldwijde onzekerheid zijn duidelijkheid en samenhang in de regelgeving strategische troeven die Europa niet langer over het hoofd kan zien. Alleen door de implementatie te vereenvoudigen, te harmoniseren en te ondersteunen kan Europa het volledige potentieel van zijn industriële digitale transitie benutten.

Voor meer informatie kunt u contact opnemen met onze Belangenbehartiger Digitalisering en Cybersecurity: Marlou Snelders (marlou.snelders@fme.nl of +31657510737).