bitkom

Position Paper

2026 February

The Future of the New Legislative Framework

Bitkom Position Accompanying the Consultation for the New Legislative Framework and Market Surveillance Regulation

The EU Commission is conducting a public consultation for the for the New Legislative Framework and Market Surveillance Regulation. This position summarizes Bitkom's core positions as a response to the consultation.

Since its introduction, the NLF has been key to efficient and fair market access in the EU. Bitkom welcomes the consultation's direction, which maintains core NLF principles: essential requirements supported by harmonised standards and a risk-based modular conformity assessment system. However, key issues remain unaddressed:

Align requirements across NLF acts. Merging NLF and market surveillance will not resolve fragmented or conflicting requirements. Real simplification requires coherent rules and NLF-consistent future legislation.

Clarify applicability to software. Definitions and processes should be updated to reflect software's specific characteristics, including its environments, rapid release cycles and digital distribution.

Ensure the legally compliant supply of spare parts. A large legal uncertainty related to circularity comes from spare parts. Components intended as spares should only need to meet the NLF rules that applied when the original product was placed on the market («repair-as-produced«).

At the same time, the consultation suggests introducing new requirements that would impose additional obligations on already compliant EU companies, while non-compliant producers or retailers are unlikely to be effectively addressed. We therefore call for a stronger focus on enforceability assessments that systematically evaluate whether proposed regulatory measures can be enforced in practice and whether they are likely to achieve their intended objectives.

Digitalisation: The DPP and the CE-Mark

Position on possible advantages, shortcomings, risks and best practices related to the possible provision of compliance information by digital means, for example, the DPP
The DPP, originally designed to support circularity, has increasingly become a key expectation for digital compliance. It is a key objective to fully digitalise processes under the NLF, including the provision of the compliance information via a DPP. However, it is important to acknowledge that this transformation will require significant investment and a redesign of processes. In particular, small companies with a currently low level of digitalisation would face an unproportionate effort and cost to achieve compliance.

Bitkom therefore strongly recommends the introduction of a DPP under the NLF, but through a step-by-step process and in close interaction with industry.

Bitkom sees two challenges:

1. **Utility**. Implementing a DPP will be costly, as companies must collect documents, convert them into uniform formats, and operate the relevant IT systems. Such a binding of a company's resources to additional bureaucracy should only be imposed if the DPP demonstrably enhances product safety in the EU. A DPP can support formal compliance by enabling automated checks to verify whether required information is complete and correct. However, preventing non-compliant products from entering the market ultimately requires strong and digitalised enforcement. Market surveillance authorities need more resources, stronger legal tools, and effective mechanisms to remove non-compliant products from online platforms. Mandatory digital reporting obligations for manufacturers will only be effective if market surveillance authorities (MSAs) are successfully digitalised in parallel.
2. **Protection of intellectual property**. Bitkom strongly advises the Commission not to include IP-sensitive information in the DPP. Technical documentation and test reports contain data that, if leaked, can severely harm competitiveness, while such documents are not essential for automated formal checks. Companies should i) be informed each time IP-protected information is accessed and ii) restrict access to a very small group of MSA staff who require it for conformity checks. We therefore recommend not making the following information mandatory in the DPP, but instead providing it upon request where required:
    - Technical documentation
    - Contents of tests and conformity assessment certificates (but not their existence), as these are additionally updated frequently
    - Repair history as it would require a product-level DPP and additional technological expenses on e.g. access management to allow repairers to edit the product DPP

Position on each product listed for online sales being accompanied by compliance information in digital form, for instance, by the DPP
Almost every product, from individuals producing handmade goods, to large-scale industrial production, is nowadays sold online. A mandatory DPP for products sold online is therefore equivalent to a mandatory DPP for all products. The same applies in the other direction: If a digital compliance tool such as the DPP does becomes mandatory (which we recommend in a gradual approach, see above), it should also accompany each product sold online.

Position on a digital CE mark
Bitkom welcomes a voluntary digital-only CE mark, as it reduces printing and design costs. This is beneficial, however, only if the various existing and planned DPP systems (the NLF digital compliance tool, the battery passport, and the ESPR DPP) are merged into a single framework so that products require only one data carrier. However, we acknowledge that the physical affixation of the CE-mark is established for many products, and that a redesign and re-organisation of processes might require a transitional period for SMEs. We therefore pledge for a voluntary digital-only CE-mark, leaving the choice to the manufacturer.

In addition, the digital labels within the DPP should not be limited to the CE mark. Instead, it should be possible to provide most mandatory physical labels, except safety labels, digitally-only.

The NLF and Sustainability

Position on additional requirements for the safety of refurbished products
Introducing additional modules for used products or substantial modifications would significantly increase the cost of circularity and should be avoided. The NLF and the Blue Guide already clarify that, after a substantial modification, conformity assessment must be carried out using the existing modules. We therefore see no need for an additional module for physical products, instead only for non-tangible software (see below). Remanufacturing is equivalent to placing a new product on the market, meaning the existing conformity assessment modules apply. Refurbishment, by definition, does not alter the safety characteristics of a product and thus does not require further assessment.

We also do not believe that a specific label for refurbished or remanufactured products would achieve the intended goals. Many products are not designed to carry an additional label, and such labels may wear off or be removed, making them unreliable, especially in the context of liability.

Position on a separate conformity assessment module for substantially modified products
The terms »substantially modified« and »refurbished« are not suitable for software, as software is subject to continuous and frequent updates. For cybersecurity and operational reasons, software products may need to be updated several times per day, with individual updates often introducing significant changes. This is now standard practice across most software development. Neither the New Legislative Framework (NLF) nor the Market Surveillance Regulation adequately reflects this reality. Applying a

hardware-based logic to software would require conformity assessments and declarations potentially multiple times per day for a single product, which is clearly unrealistic. Likewise, continuously updating technical documentation at this frequency cannot be fully automated and is therefore not feasible in practice.

The NLF should therefore move away from a hardware-centric approach for software and instead focus on the certification and documentation of development processes. This could be addressed through a dedicated conformity assessment module for software, consisting of an initial baseline assessment confirming that the software »currently meets the requirements«, combined with verification that compliance is ensured through established development processes over time. Such an approach would allow a certificate to apply to subsequent software versions, with recertification, for example, every three years.

A dedicated module of this kind would significantly improve the applicability of the NLF to software that is continuously modified.

Conformity Assessment

Position on enhanced responsibility of conformity assessment bodies
Notified bodies must apply requirements more uniformly across Europe. A consistent level of quality can only be ensured through a harmonised quality-assurance framework. We observe that differences in level of competence result from a lack of enforcement by the member states. We believe an effective measure would be to enforce the annual audits of notified bodies by their notifying authority, which are already mandatory, but not executed in all member states to the same extent:

We do not believe that reliability can be improved by imposing quantitative requirements on staff, size, or certifications. The number and capacity of notified bodies is driven by market demand. Such requirements would be counterproductive, because smaller or specialised notified bodies may no longer meet the thresholds and would drop out of the system. That might lead to a lack of notified bodies during periods of high demand, such as when new legislation enters into force.

Market Surveillance

Position on non-legislative adjustments that may be apt to boost market surveillance in the EU
We observe that previous regulatory interventions, such as the introduction of Article 6 on distance sales, have not been effective in addressing the challenges posed by e-commerce. Instead, they have created legal uncertainty and additional administrative burdens for companies. We therefore oppose any regulatory changes that would impose further obligations for European manufacturers and retailers.

The first key action is a clear and binding commitment by all EU Member States to consistently enforce existing legislation and to **provide their market surveillance authorities with adequate financial and human resources**. Only effective enforcement will allow a shift from predominantly formal conformity checks towards a genuine improvement in product safety.

To reduce the number of non-compliant products imported from non-EU countries, we consider it counterproductive to introduce additional roles or to further cascade responsibilities along the value chain. Instead, we recommend a two-step approach:

1. Prevent non-compliant products from entering the EU market: This can be effectively achieved by removing the 150 euro customs value threshold, which would require all products to be declared and registered with customs. This would provide authorities with centralised access to the information necessary to verify compliance before products are placed on the EU market.
2. Strengthen the role of the responsible person under the GPSR: This should be done by introducing more robust solvency requirements, such as proof of adequate insurance coverage and sufficient capital backing to help prevent abusive practices, including the use of letterbox companies or private individuals acting as responsible persons. One effective enforcement mechanism would be the establishment of a **central, EU-wide register of verified authorised responsible persons**, subject to clear registration criteria. Such a register would enable platforms and retailers to verify the reliability of the responsible persons associated with products offered on the market. Such a register could be accompanied by a mandatory e-Seal business wallet registration.
3. The DPP will support the retailers in identifying formally non-compliant products before placing them on the market.

Thirdly, where economic operators submit test reports or certificates demonstrating conformity with Union harmonisation legislation, issued by a conformity assessment body accredited in accordance with Regulation (EC) No 765/2008, market surveillance authorities should go beyond merely »taking due account« of such evidence. Instead, they should grant presumption of conformity with the relevant requirements to the extent covered by the accreditation scope.

Lastly, we recommend the **establishment of arbitration body on EU level** for controversial questions between Economic operators and national enforcement bodies which is separate from any EU Authority for Market Surveillance.

Position on the establishment of an EU Authority for Market Surveillance

Effective coordination across borders and across different pieces of legislation is essential, and an EU-level Market Surveillance Authority could help address existing gaps in this area. However, such an authority should not directly supervise national market surveillance bodies.

First, it is unlikely that Member States would be willing to transfer and firmly embedded national responsibilities to a central authority. Second, centralising market surveillance activities at EU level risks creating additional financial and administrative bottlenecks rather than improving enforcement efficiency.

An EU authority should therefore focus on coordination, information exchange, and guidance, while operational market surveillance remains primarily at national level.

Bitkom represents more than 2,300 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 700 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person

Vera Wesselkamp | Officer for Technical Regulation and Standardisation
P +49 30 27576-348 | v.wesselkamp@bitkom.org

Responsible Bitkom committee

WG Product Safety and Market Access