



16 November 2021

# DIGITALEUROPE position paper on the new Machinery Regulation



## Executive summary

DIGITALEUROPE welcomes the Commission's proposal for the new Regulation on Machinery Products. We are glad to see that the revision takes on board various improvements, such as increased harmonisation due to the nature of the Directive becoming a Regulation, as well as the support for digital documentation.

DIGITALEUROPE does caution however against measures that would step away from the New Legislative Framework. In this paper, we offer suggestions to improve legal certainty with the continued use of self-assessment based on harmonised standards, better alignment with AI, cybersecurity and sector-specific legislation, as well as various other points to better accommodate new technologies.

## General comments

### Conversion into Regulation

DIGITALEUROPE supports the concept of converting the Machinery Directive into a Regulation. This exercise would allow a harmonised interpretation of the legal act in all Member States and contribute towards a level playing field regarding the internal market for goods.

### Digital documentation

DIGITALEUROPE strongly welcomes the provision that instructions may be provided in digital format, especially to be able to take account of the challenges of digitalisation and the updating of instructions. This is an important modernisation that will help reduce waste as well as allow more flexible and tailored forms of documentation and up to date instructions.

In this context, we call on the Commission and legislators to take a first step here, and to look into the digitalisation of documentation and the electronic display of compliance information more generally in future initiatives as well, for instance as part of the upcoming New Legislative Framework review.

### Consensus-based standardisation

The fundamental principles of the successful New Legislative Framework (NLF) have proved central to the dual aims of protecting citizens and public interests while ensuring smooth functioning of the Single Market, thereby upholding and securing Europe's competitiveness. The efficient functioning of the European Standardisation System is vital to maintaining the integrity and strength of the NLF in support of those aims.<sup>1</sup>

The introduction of parallel approaches to standards-setting by the Commission, for instance through technical specifications, should be avoided wherever they are intended to replace standards. Such an alternative approach would only be acceptable, when used exceptionally and under strict and clear criteria, in reference to topics for which standardisation is not appropriate. The opposite would seriously harm the importance of harmonised standards and undermine the principles of standardisation.

The rules for the development of technical specifications under the proposal are neither sufficiently clear nor objective (for example, what would be considered 'undue delay' in this context). Further, technical specifications introduce the following risks:

- ▶▶ They are not based on stakeholder consensus and fail to bring to bear the broadest and deepest available expertise in their drafting.
- ▶▶ They may not reflect the latest state-of-the-art expertise and technical innovations on the market.
- ▶▶ In the absence of wider representation of stakeholders, this is less inclusive and transparent in decision-making.

The introduction of a less consensus-based alternative system to harmonised standards would lessen their global importance, create misalignments with standards developed by international standardisation organisations, and undermine the European Standards Organisations (ESO) process.

---

<sup>1</sup> <https://www.digitaleurope.org/resources/digitaleurope-views-and-messages-for-the-new-european-standardisation-strategy/>

Technical specifications<sup>2</sup> must be developed under the principles of openness to all interested parties, consensus and transparency. Sufficient expertise is necessary, which is normally provided by a high number of domain experts. These conditions are met when the specifications are developed by ESOs (CEN, CENELEC and ETSI).

DIGITALEUROPE proposes that the Commission, in conjunction with ESOs and industry, develops a clear set of rules establishing the compelling exceptional circumstances in which a technical specification would be justified. They should also provide that they be retired once suitable harmonised standards become available. These rules should also address how suitable domain experts can contribute to the content of the technical specification.

### **Transitional period**

The proposed Regulation introduces significant changes to the conformity processes (see below). DIGITALEUROPE requests a transitional period for 30 months after the date of entry into force of this Regulation, machinery which complies with the provisions of the existing Machinery Directive shall also be considered to be in compliance with this Regulation. This would allow manufacturers to continue to place their machinery products on the market under the existing Machinery Directive, while updating their processes and workflows for the new Machinery Regulation.

## **New requirements & obligations**

### **Mandatory 3<sup>rd</sup> party conformity assessment**

The proposed Regulation introduces a new category of 'high-risk' machinery products, listing these out in its Annex I. These existing products were not treated differently before. A noteworthy addition is that of software and AI system ensuring safety functions in combination with the introduction of mandatory 3<sup>rd</sup> party conformity assessments, a departure from established practice.

The provisions in the existing Machinery Directive, as well as is normally the case in most NLF legislation, allow manufacturers to use self-assessment and self-declaration of machinery products, where suitable harmonised standards are listed in the Official Journal. These harmonised standards cover all the relevant essential health and safety requirements, in practical terms for manufacturers to implement.

---

<sup>2</sup> As in the overall New Legislative Framework, as set up by Decision 768/2008/EC and referenced to in Annex II 3(a)-(c) of Regulation (EU) 1025/2012.

This approach has proved satisfactory for many years, covering all machinery products, including those that would now be considered under the new high-risk category. The Regulation instead proposes 3<sup>rd</sup> party conformity assessments, instead of self-declaration and self-assessment. This means that companies would need to have their products tested again, against the same harmonised standards for health and safety requirements, adding costs and delays in time to market (of at least several months).

Requiring such 3<sup>rd</sup> party conformity assessments would therefore certainly make the rollout of new machinery much more burdensome and make the overall compliance assessment process much less predictable.

DIGITALEUROPE however sees no reasoning why the established procedure would need to be changed, or why such a new categorization is required in the first place. The Commission has insufficiently demonstrated why this change from the existing practice of the past decades, or why mandatory 3<sup>rd</sup> party conformity assessments would benefit users.<sup>3</sup>

Consequently DIGITALEUROPE strongly urges the legislators that, in absence of a clear and evidenced justification behind the change of approach, the option for self-assessment is retained. Any 3<sup>rd</sup> party conformity assessment procedure should be strictly limited to cases where the existing, established practice has proven to be insufficient in addressing health and safety risks.

### Control systems

DIGITALEUROPE believes that the proposal for machine builders to consider malicious attempts from third parties in creating a hazardous situation<sup>4</sup> is not possible to foresee as this requires knowledge of future malicious attempts (such as zero-day exploits).

DIGITALEUROPE recommends that the Regulation only applies to those risks that are known when the equipment is placed on the market<sup>5</sup> or put into service. State-of-the-art cyber security standards can be applied at the time the equipment is placed on the market or put into service, but not beyond that point.

---

<sup>3</sup> See also the opinion and response to the public consultation on the review of the Machinery Directive by CEN-CENELEC: [https://www.cencenelec.eu/media/Policy%20Opinions/2021-07-07\\_cen-cenelecpositionondraftmachineryregulation.pdf](https://www.cencenelec.eu/media/Policy%20Opinions/2021-07-07_cen-cenelecpositionondraftmachineryregulation.pdf)

<sup>4</sup> See Annex III EHSR 1.2.1 (safety and reliability of control systems), point (a) on malicious attempts from third parties.

<sup>5</sup> The element of 'making available' can occur many times, and long after the product has been 'placed on the market' – especially for safety components.

This is particularly important for safety components which may be placed on the market some time before the final machine product itself is placed on the market or put into service.

### **New digital technologies & Autonomous mobile machinery**

DIGITALEUROPE would like to stress that the existing essential health and safety requirements of the Directive are technology-neutral. This allows them to be applied regardless of technological changes or advancements.

The essential requirements listed in the Regulation's Annex III should therefore remain technology-neutral and should not be overly prescriptive, as European manufacturers depend on the NLF principles, whereby the essential requirements are laid down in product legislation and the technical realisation is detailed in product specific voluntary standards reflecting the state-of-the-art.

Examples of essential requirements being too prescriptive are the provisions for autonomous mobile machinery and machinery with evolving behaviour. Contrary to the Commission's goal to better accommodate autonomous mobile machinery, the proposed requirements would restrict autonomy instead of enhancing it. For instance, the proposed supervisory control would be limited to starting or stopping the machinery, while many other functions could be useful (e.g. slowing down, return to base).

It also requires that the operator has full visibility of the machinery's operation and surroundings. This would in practice not be possible, to assess what this all would need to entail or to guarantee this at all times (e.g. to allow the machinery to continue safe operation in case of a break in network connection).<sup>6</sup>

Similarly, the updated 'driver' definition as proposed by the Commission seeks to remedy the lack of clarity for the rollout of autonomous mobile machinery caused by the notion that all mobile machinery must have a 'driver'. However, the proposed wording would require applying all driver-related EHSRs that are not obviously limited to drive-on drivers also to autonomous mobile machinery.

For example, section 3.2.1 requires that the 'driver' has sufficient visibility to operate the machinery safely from the driving position. Similarly, section 3.3.1 requires that the 'driver' must be able to actuate all control devices required to operate the machinery from the driving position. As autonomous mobile machinery is not excluded from these provisions, this could effectively restrict their autonomy.

We therefore suggest moving details on the remote supervision to the new definition for autonomous mobile machinery instead of including them in the existing 'driver' definition.

---

<sup>6</sup> See Annex III, Supplementary EHSR 3.2.4

Further, the proposed rules for machinery products with evolving behaviour seem to be tailored towards humanoid robots and envisage such type of interaction and communication.

For instance, the Regulation specifies that such machinery products should be able to respond through “*words,[...] and gestures, facial expressions, or body movement*”.<sup>7</sup> The phrasing of this provision however implies it would also apply to any type of machinery product with evolving behaviour or some level of autonomy. That would include many other types of machinery products that do not have such an interaction or would be incompatible with the listed requirements.

## Coherence with other legislation

### Alignment with the New Legislative Framework (NLF)

DIGITALEUROPE supports the alignment with the New Legislative Framework (NLF) as it provides coherence with other product safety legislation<sup>8</sup>. It is also essential that coherence with ongoing legislative proposals concerning AI and cyber-security is ensured, as European manufacturers depend on seamless EU conformity and market access regulations for their success.

The Machinery Regulation further includes many references to health and safety requirements (formulated as “*the health and safety of persons and, where appropriate, domestic animals and property and, where applicable, the environment*”), which imply requirements that are not correspondingly covered in the essential requirements of Annex III. For objective clarity and certainty, those references should be directed instead to the essential requirements. Where such further requirements exist, they should be incorporated into the essential requirements of Annex III.

There are also some detailed deviations from the NLF text that, taken together with other concurrent legislative proposals, aggregate to significant and fragmented deviations from the NLF, thereby weakening its standing as an harmonised framework. This should be avoided.

---

<sup>7</sup> See Annex III EHSR 1.1.6, 1.3.7

<sup>8</sup> Including the Radio Equipment Directive, General Product Safety Directive, Low-Voltage Directive or the more sector-specific Medical Devices and In-Vitro Diagnostics Regulations.

Examples of provisions which should be removed then include<sup>9</sup> those mandating an email address in addition to the postal contact address<sup>10</sup> and potentially requiring translated/rescripted versions of labelled contact details.

### Definition of AI & AI systems ensuring safety functions

The proposed definition of an AI system would include broadly used and well established industrial ‘conventional logic units’ without any AI software, resulting in unjustifiable additional burdening and increased obligations.

DIGITALEUROPE proposes that the Machinery Regulation specifies that conventional logic units (without AI software) are not listed as AI systems when these units utilise embedded or application software that is developed using hard-coded and rule-based software systems.

Additionally to the broad definition of AI itself, the Machinery Regulation’s Annex I has an overly broad scope which would result in all safety devices utilising software being declared as ‘high-risk’. It basically considers any safety function that incorporates software somehow (which, currently, is nearly always the case except purely passive devices) as inherently risky.<sup>11</sup>

The scope should rather be limited to software ensuring safety functions that embeds an AI system, aligning it also better with the proposed AI Act. DIGITALEUROPE consequently recommends that Annex I’s item 24 is amended to “*AI systems ensuring safety functions*” and the deletion of item 25. Similarly item 18 in Annex II should be amended to “*AI systems ensuring safety functions*”

### Cybersecurity

The inclusion of requirements on cybersecurity<sup>12</sup> in the more sector-specific Machinery Regulation is not considered appropriate, as only individual sectors are affected. This will lead to inconsistent and contradictory requirements.

Further, the collection of evidence for both hardware and software components will pose technical problems and result in significant additional costs with no associated benefits.

The Machinery Regulation should therefore not specifically address cyber threats and, rather than relying on provisions in vertical or sectorial legislation,

---

<sup>9</sup> Both in art. 10(6)

<sup>10</sup> Both email and website address are normally not required under the well-established Blue Guide reference document for NLF compliance. It should also be noted that proper resourcing and coordination of market surveillance authorities should be prioritized, to utilize the toolset and information already at their disposal.

<sup>11</sup> See Annex I, items 24 and 25

<sup>12</sup> See Annex III EHSR 1.1.9 and 1.2.1

DIGITALEUROPE recommends that concerns regarding cybersecurity are addressed through a product-related horizontal legal act on cybersecurity in accordance with the principles of the NLF.

### Meaningful exemptions for already highly-regulated sectors

While the Commission has included certain exemptions, we remain concerned that the provisions for so-called ‘high-risk’ machinery under the Directive would nevertheless create a duplication of sector-based requirements for highly-regulated industries in practice.

For instance, this is the case for automobiles and their systems and equipment that are subject to EU type-approval. Included within Article 2 (2)(e) of the General Provisions of the proposed Regulation is an exemption for “*vehicles which have as their only objective the transport of goods or persons by road, air, water or rail except for machinery mounted on those vehicles*”. With regard to autonomous vehicles, the machinery in question is due to be regulated as part of an Implementing Act to the General Safety Regulation (2019/2144) that will be in place by 6 July, 2022.<sup>13</sup>

This means that the whole autonomous vehicle will be subject to type-approval rules, where regulators will need to assess the safety and performance of both the system and its physical components together. Since this exemption has been created in order “*to prevent that vehicles not covered by that legislation are covered by default by the machinery legislation, as this legislation is not meant to regulate risks other than those stemming from the machinery function*”, DIGITALEUROPE proposes that machinery already subject to type-approval be exempt from the requirements of the Regulation.

## Other elements

### Disclosure of the source code

Explicit reference of “*source code or programmed logic*” to be included in the technical documentation<sup>14</sup> will lead regulators more quickly demanding its disclosure, which would affect highly sensitive business secrets – without particular benefit in most cases. This point is also particularly relevant in connection with the broad provisions on data sharing between national regulators in the EU and third countries.<sup>15</sup>

---

<sup>13</sup> <https://circabc.europa.eu/ui/group/4273d650-b8a9-4093-ac03-18854fbba4b5/library/0544523b-df3a-4295-9b22-80d271af8f1f/details>

<sup>14</sup> See art. 10(3)

<sup>15</sup> See art. 47

The Regulation should not specifically ask for the disclosure of the source code and let the competent authorities tailor their information request to verify conformity of machinery. A reasoned request must include the justification on the grounds of the adequacy and proportionality of the type of information they are requesting, and would like to see additional safeguards as to the exchange of information among national authorities.

### Logging and data retention

The requirements for tracing logs and security-related data recording are unclear and create burdensome compliance efforts.<sup>16</sup> For instance, to what extent these obligations fall on the machinery product's user, which would lead to significant data safety and confidentiality concerns if the manufacturer is expected to be the one to retain all relevant logs and data. The scope of such retention obligations should be clarified and limited.

Further, the proposed and possibly constantly renewed retention periods<sup>17</sup> should be limited due to the potentially vast amounts of data. We recommend that the appropriate retention periods, and selection of which data to log, to harmonised standards or to the manufacturer's case-by-case risk assessment.

### Use of virtual testing data

Virtual testing means replacing one or more physical elements characterized by a digital simulation model. The goal of such virtualization is to resemble, to a sufficient extent, the original physical elements. Consequently, it can be used to reduce the burden of physical tests and effectively provide evidence of a system's performance across the entire operational domain. Virtual testing provides a powerful tool to assess the performance of a system under diverse, safety critical or complex conditions which would otherwise not be practical for conventional physical testing.

For machinery applications, virtual testing can be used to reproduce either the entire system, a subsystem, or a component (e.g. a sensor). No one virtual testing tool can be used to test all aspects of the machine, this is why manufacturers may exploit the attributes of various virtual testing tools to develop confidence in the safety of the full system.

Through this approach, an assessor can get confidence about the machinery based on the virtual tests performed by the developer in an agile, controllable, predictable, repeatable, and efficient manner. While robust virtual test methods

---

<sup>16</sup> See Annex III, EHSR 1.2.1

<sup>17</sup> Annex III EHSR 1.2.1 (f) specifies five years for software updates, while (g) specifies one year from placing on market for other cases.

are available and widely used, this revision and proposed Machinery Regulation should be an opportunity to offer more explicit provisions that support the use of virtual testing to generate data for the manufacturers conformity assessment.

DIGITALEUROPE recommends therefore to make the proposal more innovative and future proof, and that Annex IV A (o) is amended to include the underlined addition “*for sensor-fed, remotely-driven, or autonomous machinery product, if the safety related operations are controlled by sensor data, a description, where appropriate, of the general characteristics, capabilities and limitations of the system, data, development, testing (physical or virtual) and validation processes used [...]”.*

## Conclusion

In this paper, we’ve outlined our proposals to further improve the proposed Machinery Regulation. The general comments as well as targeted amendments should strengthen the role of the Regulation within the New Legislative Framework, and be better equipped to deal with both the challenges and opportunities stemming for new digital technologies.

DIGITALEUROPE looks forward to engage further with policy-makers in the continuing legislative discussions and negotiations on this file.

FOR MORE INFORMATION, PLEASE CONTACT:



Jochen Mistiaen

**Senior Policy Manager**

[jochen.mistiaen@digitaleurope.org](mailto:jochen.mistiaen@digitaleurope.org) / + 32 496 20 54 11

## About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

# DIGITALEUROPE Membership

## Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

## National Trade Associations

**Austria:** IOÖ

**Belarus:** INFOPARK

**Belgium:** AGORIA

**Croatia:** Croatian Chamber of Economy

**Cyprus:** CITEA

**Denmark:** DI Digital, IT BRANCHEN, Dansk Erhverv

**Estonia:** ITL

**Finland:** TIF

**France:** AFNUM, SECIMAVI, numeum

**Germany:** bitkom, ZVEI

**Greece:** SEPE

**Hungary:** IVSZ

**Ireland:** Technology Ireland

**Italy:** Anitec-Assinform

**Lithuania:** INFOBALT

**Luxembourg:** APSI

**Moldova:** ATIC

**Netherlands:** NLdigital, FIAR

**Norway:** Abelia

**Poland:** KIGEIT, PIIT, ZIPSEE

**Portugal:** AGEFE

**Romania:** ANIS

**Slovakia:** ITAS

**Slovenia:** ICT Association of Slovenia at CCIS

**Spain:** AMETIC

**Sweden:** TechSverige, Teknikföretagen

**Switzerland:** SWICO

**Turkey:** Digital Turkey Platform, ECID

**United Kingdom:** techUK