ETUC call against postponement of the application of cybersecurity and AI-related provisions in the Machinery Regulation (EU) 2023/1230

The ETUC is against postponing the application of requirements on cybersecurity and AI provisions of the Machinery Regulation.

The proposal to postpone these requirements was presented by several industry associations to the EC Machinery Expert Group (MEG). Their call (document 11.5) requests two postponements:

- Postponement of the application of the independent conformity assessment procedures requirements concerning AI systems (items 5 and 6 of Annex I, Part A of the Machinery Regulation) by at least 24 months after the finalisation of the topic in the EC Guide to the application of the machinery legislation.

- Aligning the date of the application of the requirements EHSR *1.1.9 Protection against corruption* and EHSR *1.2.1 (f) Safety and reliability of control systems* of Regulation (EU) 2023/1230 with the date when the Cyber Resilience Act comes into effect (11 December 2027).

We strongly oppose this request for several reasons.

The request to postpone the conformity assessment procedures on machinery using AI by a notified body, will cause more uncertainty and most likely non-compliance of machinery. We would like to highlight that machinery using AI as a safety function are considered high-risk, as noted in Annex I, Part A, for a reason. Therefore the need to assess their conformity with the respective requirements by a Notified Body is of crucial importance for guaranteeing the safety of working with these machines. At the same time, we find the Machinery Regulation and in particular Annex I is clear as it defines and sufficiently lays out the requirements for the machines using self-evolving behavior.

We would like to remind as it was explained at the Machinery Expert Group meeting, that the existence of harmonised standards is not a prerequisite for the accreditation of Notified Bodies to run conformity assessment for machines using AI. In the absence of standards, the Notified Bodies are being accredited following a review of procedure aligning to the technical state of art, ensuring the staff is competent, demonstration on test models and gathering information from manufacturers from machines using AI.

The joint industry paper refers to the interpretative work on the EC guide for application of the Machinery Regulation and its role in providing further information on the requirements for machinery using AI in a safety function. We would like to highlight that the update of the EC guide should only provide clarification on the basis of what is in the regulation, but should not interpret or provide any information beyond. As such, the information needed is already provided in the regulation.

We also call for caution to link the application of the requirement for conformity assessment with the finalization of the EC Guide. It would postpone, if not suspend, the conformity assessment by an unknown time. While the joint industry paper proposes 24 months after the Guide has concluded on this, there is no saying when the Guide will be ready. The work is already delayed and long discussion could even further hinder the finalization of the work. This should not be used as an excuse to postpone the application of the regulation.

On the request to postpone the requirements on cybersecurity, we would like to point out that the requirement that a machine that can be accessed remotely must be free of security vulnerabilities is not new. In fact, this has been known for years over the process of the revision of the machinery legislation. We fear that companies that have been unable or unwilling to implement the required measures since the announcement of the revised Regulation will also not do so when given more time. A postponement weakens the European market because workers, users and customers assume that a product is security-compliant whereas it may not be.

In addition, delays at testing centres and end customers would lead to greater uncertainty. A product compliant with the Machinery Regulation would be sold in February 2027 without protection against corruption, and two years later it would be almost impossible for retailers and users to tell which products are compliant and which, under the old transitional rules, do not meet the higher requirements for AI and protection against corruption. The Cybersecurity Resilience Act does not fully cover these requirements.

Hence, the **postponement of the conformity assessment for machines using AI and of the requirements on cybersecurity is not necessary**. On the contrary, the increasing use of machines with self-evolving behaviour and machines that can be accessed remotely, as well as the increased risk to safety when working with them calls for the need to equip and assess them according to the safety requirements of the regulation. A postponement would mean postponing the level of safety needed to work with machines.

Background

Machinery safety is a key element of occupational health & safety, which is one of the core demands of the ETUC and its affiliates: national unions and European union federations. Many workers across different sectors work with machines: on industrial and construction sites as well as in agriculture. Technical protective measures increasingly depend on networked control systems. In order for these to be able to protect against danger, they must themselves be protected against corruption. Cybersecurity threats—such as hacking, manipulation of control systems, or unsafe remote operation—can directly compromise a machine's safety. At the same time, the use of AI in safety-related functions may create unpredictable or erroneous behaviour if not properly designed, tested, and monitored. As software becomes central to

machinery performance, it is essential to ensure robust protections so that workers remain safe in the face of these emerging digital and AI-related risks.

The Machinery Regulation (EU) 2023/1230 addresses this by modernising the safety framework for machinery placed on the European market and expressly addresses emerging technological risks, including cybersecurity and the use of artificial intelligence. It introduces mandatory requirements to ensure that machinery incorporating digital controls is designed to withstand cyber-attacks that could compromise safety-related functions. When AI systems are used as part of a safety function, the Regulation subjects the machinery to an independent conformity-assessment by a notified body. These rules aim to ensure that adaptive or data-driven technologies are robust and do not introduce unpredictable behaviour that could endanger workers or end-users, thereby aligning machinery safety with the EU's broader digital and AI regulatory framework.

The ETUC is the voice of workers and represents 45 million members from 94 trade union organisations in 42 European countries, plus 10 European Trade Union Federations. The ETUC is a member of the MEG.