EUROSMART
The Voice of the Digital Security Industry

# Revision of the Machinery directive

## Answer to the European Commission public consultation

Eurosmart, the voice of the digital security industry represents manufacturers of secure elements, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers, as well as laboratories and Technical inspection companies. This community of European actors is deeply involved in providing trustworthy solutions to complete the European Digital Single Market.

Europe benefits from world-leading industry and know-how in the fields of machinery manufacturing and industrial IoT. Artificial intelligence and IoT are game-changing technologies which make an evolution of the Machinery directive a real necessity. For these reasons Eurosmart welcomes the European Commission initiative to consult stakeholders.

By 2025, the projected IoT connections are expected to exceed the 25 billion of units' threshold [1]. In the meantime, industrial IoT devices will account for over half of these connections. One can expect a fast expansion of internet connected machinery. 'New approach' principles which sets mandatory basic requirements which are to be underpinned by a European Standardisation approach, is a prerequisite to make the concerned European legislative corpus, fully compliant with the digital age and market's needs.

Eurosmart enjoins the Commissions to fulfil some key principles for safeguarding the European actors, ensuring a high security and safety level for consumers while making Europe a market of excellence where global manufacturers are expected to provide their safer products.

## Artificial intelligence should be tackled out of the scope of the Machinery Directive

According to the High-Level Expert group on Artificial intelligence set up by the European Commission, AI systems are software (and possibly also hardware) systems […] interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI Systems aim to interact with "cyber-physical systems", which have an impact on safety of the machinery where AI has been integrated.

Due to the critical nature of AI which could be considered as a piece of software possibly embedding a piece of hardware, high level cybersecurity rule should apply in terms of privacy, data processing, security by design and by default. Eurosmart recommends the European Commission to deals with AI through specific rules outside the scope of the review of Machinery directive which aim to introduce basic security requirements.

## Machinery Directive within the New Legislative Framework

Eurosmart acknowledges the benefits in terms of safety of the New Legislative Framework (NLF) approach which provides flexibility for manufacturer and set out a same level-playing-field between manufacturers and importers.

For these reason Eurosmart welcomes the idea of an alignment of the directive with the NLF. This framework ensures consistency amongst the member states, for the procedures of product conformity assessment. To correctly address the cybersecurity part of the conformity assessment, a particular attention must be paid to the appointment and to the monitory of Notified bodies by the Member States, the process can still be improved. The transformation of the directive into a regulation would ensure a better implementation and facilitate the uniformisation of the rules.

However, the NLF has not been built to assess a resistance level of products to potential cyber-attacks. Cybersecurity third-party evaluations which are risk-based approaches, do not follow the same procedures as the safety ones do. This is particularly true, when it comes to the necessary penetration testing for cybersecurity evaluations. Nevertheless, conformity assessment could be convenient for industries to attest a basic level of security requirements.

## An affordable solution for market actors is needed

Applying basic security requirements won't bring any exaggerated additional costs for manufacturers. According to their maturity level, most of the European manufacturers have already integrated them (privacy by default). Raising up the security level for placing a product on the European Market will create market opportunities and incentives - if the process remains simple, efficient, and enough flexible to be implemented -. As a complement, SMEs should be accompanied to address these new cybersecurity requirements, it could be an opportunity to differentiate themselves by gaining a unique know-how and to compete on the global stage.

## An entry point to reach higher security levels

Mandatory basic security requirements would be beneficial to the European market and to ensure consumers with minimum security level which is directly linked to cyber-hygiene. Several ways should be explored and based on European and national standardisation organisations: ie ETSI TS 103-645 or DIN TS. All new requirements must be based on the ESOs work to ensure European strategic autonomy in Cybersecurity and to avoid importing external solution that could bring external dependencies.

The requested cybersecurity evaluations must be performed by a third party, self-assessment is not appropriate to reach enough level of trust and security, even if it's based on a certification process.

## Consistency with other EU Cybersecurity legislative initiatives

These mandatory basic security requirements are somehow a baseline approach and shouldn't deter the market to address higher security levels. Eurosmart strongly recommends a risk-based approach when it comes to cybersecurity evaluation, and higher security levels are necessary to concretely improved the resistance level to potential attacks in specific environments. To achieve this goal links should be created with the European Cybersecurity Certification Framework for substantial and high levels. A product which has been certified by a European Scheme should benefit from a presumption of conformity with mandatory basic security requirements.

In addition, the general data protection regulation foresees certification in terms of privacy. The European legislator should avoid piling requirements on certifications. A consistency amongst all the mandatory and voluntary cybersecurity certification and other requirements addressing products, services and process should be ensured in a flexible manner.

## About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

## Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (**BCA**, **Fingerprint Cards**, **Gemalto**, **Giesecke+Devrient**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Internet of Trust**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **Trust CB**, **WISekey**, **Winbond**), laboratories (**Keolabs**, **Serma**, **Brightsight**, **Red Alert Labs**, **Cabinet Louis Renaud**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com

@Eurosmart_EU

@Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | mail eurosmart@eurosmart.com