Unlocking life-saving innovation: ENSHPO response to the digital fitness check call for evidence

Roberto Sammarchi, Attorney at Law, PhD, LLM
AIAS (IT) representative in ENSHPO

Executive summary

The European Network of Safety and Health Professional Organisations submits this comprehensive analytical report in response to the European Commission's Call for Evidence regarding the Digital Fitness Check. The evaluation of the cumulative impact of the European Union's digital rulebook on competitiveness, innovation, and strategic autonomy is a timely and strictly necessary exercise.

The current regulatory architecture establishes a globally recognized standard of protection. However, the Commission has rightfully identified the need to assess how different laws work together, identifying synergies, good practices, and any remaining gaps, overlaps, and inconsistencies. This response articulates a strategic blueprint to transition the regulatory framework from a defensive posture to an enabling ecosystem. The core argument posits that a regulatory environment designed to protect citizens is inadvertently creating a chilling effect on the very technologies engineered to save lives in the workplace.

To resolve these inconsistencies and ensure the framework remains effective, proportionate, and fit for the future, this contribution advocates for a calibrated application of derogation clauses to distinguish between invasive surveillance and protective monitoring. It strongly supports the targeted amendments introduced by the Digital Omnibus, particularly the consolidation of the data legislative acquis and the establishment of a single-entry point for cybersecurity incident reporting. Furthermore, it evaluates how to align the protection of personal data with the fundamental right to safe working conditions, proposing practical pathways for occupational safety and health professionals.

Assessing the cumulative impact on competitiveness and innovation

The European Union's digital acquis is constructed upon essential principles designed to protect citizens, ensure fair market dynamics, and establish global standards for ethical technology deployment. However, evaluating how this rulebook affects the competitiveness objective of the EU reveals significant challenges. The cumulative compliance burden risks pricing small and medium enterprises, as well as small mid-cap companies, out of the internal market. These smaller entities form the backbone of specialized occupational safety and health technological development, providing tailored solutions for high-risk industrial environments, construction sites, and manufacturing plants.

The total cost of complying with the complex web of digital regulations across the European economy is projected to reach billions of euros over the next five years. For many systems, these costs are compounded by mandatory third-party conformity assessments, adding significant expenses and delays to market entry. This dynamic penalizes developers of protective technologies and creates a perverse incentive for employers to maintain traditional, less effective safety protocols rather than investing in advanced digital prevention. Painting lines on a warehouse floor remains a cheap compliance measure, whereas installing an advanced computer vision system to prevent vehicle-pedestrian collisions triggers a cascade of regulatory obligations under multiple overlapping frameworks. The Digital Fitness Check must ensure that compliance costs do not act as an insurmountable barrier to life-saving innovation, allowing the EU to remain a competitive leader in industrial safety.

Identifying synergies and good practices: A foundation to build upon

The Call for Evidence explicitly seeks the identification of synergies and good practices within the current framework. The recent Digital Omnibus proposal demonstrates a clear understanding of these needs and introduces several excellent practices that should be systematically expanded.

The proposal to establish a single-entry point for incident reporting, managed by the European Union Agency for Cybersecurity, is a prime example of a positive regulatory synergy. By allowing entities to fulfill overlapping reporting obligations under the NIS2 Directive, the General Data Protection Regulation, the eIDAS Regulation, the Digital Operational Resilience Act, and the Critical Entities Resilience Directive through a single interface, the Commission is drastically reducing administrative redundancy.

Another vital good practice is the extension of simplified compliance measures and

regulatory privileges, initially designed for micro and small enterprises, to small mid-cap companies. By recognizing that entities slightly larger than traditional medium-sized enterprises still face structural disadvantages compared to large tech conglomerates, this extension fosters a more competitive environment for specialized European software developers focusing on industrial safety. These synergies prove that high regulatory standards can coexist with streamlined administrative processes.

Addressing gaps, overlaps, and inconsistencies

Despite the positive steps taken, significant gaps and inconsistencies remain at the intersection of various digital laws, particularly concerning the deployment of safety technologies.

The Artificial Intelligence Act introduces a risk-based approach that classifies systems intended for employment, management of workers, and access to self-employment as high-risk by default under Annex III. From a functional standpoint, this broad definition captures a vast range of beneficial occupational safety technologies. The regulatory framework currently omits a clear distinction between invasive surveillance, used for administrative or disciplinary management, and protective monitoring, engineered exclusively to detect fatigue, identify environmental hazards, or prevent machinery accidents.

The legal uncertainty surrounding the derogations in Article 6(3) may force developers to assume the high-risk classification to avoid severe administrative fines. To resolve this, a systematic application of these derogations is necessary. Systems designed purely for risk reduction, such as emergency stop mechanisms or biometric fatigue detectors, which do not introduce new threats to fundamental rights and are technically isolated from performance evaluation metrics, should benefit from these derogations. Furthermore, to ensure legal certainty, it remains important to foster a harmonized interpretation of the regulatory scope across all Member States. A consistent understanding of advanced algorithmic capabilities will prevent fragmented enforcement and provide developers of occupational safety technologies with the predictability required to scale their solutions EU-wide.

A fundamental overlap and tension also exists between the data minimization principle enshrined in Article 5 of the General Data Protection Regulation and the technical requirements of predictive safety analytics. Developing reliable predictive safety models requires extensive, high-frequency, and multivariate datasets. In the context of real-time safety systems, true and irreversible anonymization is frequently impossible without destroying the utility of the data. A system designed to halt machinery must precisely identify the specific individual in danger to trigger a targeted alert; aggregating this data renders the life-saving function entirely

inoperative.

The targeted amendments proposed in the Digital Omnibus provide an opportunity to alleviate this friction by clarifying situations involving the residual processing of special categories of personal data for the development and operation of algorithmic models.[2] By stipulating that such processing is permissible provided the controller implements appropriate technical and organizational measures to prevent the disclosure of special categories of data, the Omnibus offers a pragmatic pathway for developers of safety analytics.

Ensuring the system is effective, proportionate, and fit for the future

To ensure the digital rulebook is fit for the future, it must be adaptable to rapid technological evolution. The integration of complex algorithmic systems, wearable sensors, and collaborative robotics into professional practice necessitates a proactive and agile regulatory approach.

The European Commission should issue a formal standardization request to the European Standards Organisations to develop specific harmonized standards for occupational safety applications. Adherence to these standards would provide a presumption of conformity, drastically reducing the compliance burden and accelerating the deployment of protective equipment.

Furthermore, future-proofing the ecosystem requires the establishment of specialized regulatory sandboxes dedicated to occupational safety. These environments would serve as safe harbors, allowing innovators to test protective technologies collaboratively with competent authorities, worker representatives, and social partners. Testing in these controlled environments shields developers from the immediate threat of administrative fines, accelerating the transition from prototype to market-ready life-saving applications.

Finally, to ensure effective human oversight in the future, the establishment of a formal certification for safety professionals, such as a Certified AI Safety Professional designation, is highly recommended. This would empower professionals to audit algorithmic fairness and validate the physical safety parameters of deployed systems.

Delivering on the high standard of protection of fundamental rights

The Digital Fitness Check aims to ensure the digital rulebook delivers on the EU's high standard of protection of fundamental rights. In the context of the workplace, this requires a delicate balancing act. Article 31 of the Charter of Fundamental

Rights of the European Union guarantees every worker the right to working conditions which respect their health, safety, and dignity.

Currently, the strict interpretation of privacy rules can sometimes inadvertently conflict with the fundamental right to physical safety. Relying on employee consent as a legal basis for processing safety data is legally fragile due to the inherent imbalance of power in the employment relationship. The appropriate legal basis for deploying protective monitoring technologies must be the employer's legal obligation to ensure health and safety.

The regulatory framework should explicitly recognize and incentivize the use of Privacy-Enhancing Technologies to reconcile these fundamental rights. Solutions such as federated learning, where models are trained on decentralized data without raw data leaving a local device, and synthetic data generation offer effective means to build highly accurate safety models without centralizing sensitive personal information. By promoting these technologies, the EU can protect the fundamental right to data protection while simultaneously upholding the fundamental right to a safe working environment.

Conclusion

The digital rulebook must transition from a purely defensive posture to a framework that actively enables beneficial technology. The Digital Fitness Check offers an indispensable mechanism to evaluate the coherence, efficiency, and proportionality of the European Union's regulations. By addressing the identified gaps in risk classification, expanding the excellent synergies proposed in the Digital Omnibus, and clarifying the interplay between data protection and physical safety mandates, the European Commission can unlock life-saving innovations. Ensuring that these rules are streamlined, clear, and fit for the future will elevate the standard of occupational safety and health across the continent while reinforcing the global competitiveness of European enterprises.