

TOWARDS TRANSPARENCY: SMART DIGITAL SYSTEMS FOR IMPROVING WORKERS' SAFETY AND HEALTH

Smart digital systems for improving workers' safety and health¹ are systems using digital technologies to collect and analyse data to identify and assess risks, prevent and/or minimise harm, and promote occupational safety and health (OSH).²

Often, these systems are based on data collection devices, such as sensors, cameras, microphones, etc., which transmits data via Bluetooth, radio-frequency identification or the Internet of things to a cloud platform. In the case of the latter, artificial intelligence (AI) and machine learning (ML) algorithms process data and translate it to information that employers can use to prevent or react to risks. Of course, there are other options too: from smart monitoring systems using augmented reality, virtual reality or mixed reality to train workers in high-risk sectors, to drones conducting remote inspections in the real estate, construction, oil and gas³ or rail sector, these systems are increasingly entering the workplace, and changes conditions for management of safety.

Research conducted by the European Agency for Safety and Health at Work's (EU-OSHA) suggests that companies and organisations can improve the safety and health of their workers using these systems.⁴ However, certain conditions should be met. These include embedding the smart digital systems in existing OSH framework instead of using them to replace it, and understanding that together with benefits, the smart digital systems can come with limitations.

Further EU-OSHA's research shows that workers' involvement is an important condition for the effective implementation of smart digital systems. There is a need to ensure that workers are fully on board when their employer introduces new monitoring technology. It is vital that employers address workers' concerns around the potential use of these systems. Such concerns typically revolve around the potential transfer of responsibility for safety and health from employers to workers, as well as the possibility of the use of the data collected for performance measurement, and the resulting potential negative implications for workers.

The issue of data privacy

Privacy of personal⁵ or sensitive⁶ data is one of the most critical issues in the debate around the use of smart digital systems at the workplace. One of the main concerns in relation to data privacy is the potential misuse of workers' data for performance measurement, which could then be used as grounds for discrimination, or, cases of unfair dismissal.

An example of this would be a smart monitoring system in a warehouse that tracks workers' physical and physiological characteristics. Such a system could identify workers with elevated heart rates or high stress levels, which means that they could be flagged as potential liabilities for the business. This in turn could lead to discrimination, for example, in terms of promotions, or the dismissal of the worker.

¹ The term is used interchangeably with 'new OSH monitoring systems' and 'smart monitoring systems'.

² EU-OSHA – European Agency for Safety and Health at Work, *Smart digital monitoring systems for occupational safety and health: uses and challenges*, 2023. Available at: <https://osha.europa.eu/en/publications/smart-digital-monitoring-systems-occupational-safety-and-health-uses-and-challenges>

³ EU-OSHA, Drones inspecting worksites of gas infrastructure operator (ID16) Available at: <https://healthy-workplaces.osha.europa.eu/en/publications/drones-inspecting-worksites-gas-infrastructure-operator-id16>

⁴ Ibid.

⁵ European Commission. (n.d.). *What is personal data?* https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

⁶ European Commission. (n.d.). *What personal data is considered sensitive?* https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

While these might be extreme examples, it underscores the importance of safeguarding workers' data, as well as of ensuring that their use is exclusively for safety and health purposes. It also shows how difficult the issue can be, in particular when grappling with challenging questions. For example, there are concerns whether it is possible to establish a threshold for psychosocial factors, such as how much "stress" is acceptable at a workplace. This is complicated further by the fact that individuals have different thresholds for stress. Additionally, there are issues such as the accuracy of collected data and the processes that govern their interpretation.

Drawing on real-world examples, this policy brief presents practical ways in which manufacturers or developers of smart OSH monitoring systems and their clients, the deployers⁷(employers), can address issues around data privacy and develop tools to promote workers' health and safety.

Privacy by design

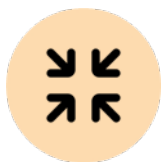
Embedding privacy by design appears to be one of the most effective ways to address data privacy. Some practical ways in which manufacturers or developers could work in this direction include the following:

Figure 1: Privacy by design



Anonymisation

Anonymising personal data by, for example, assigning unique identifiers instead of worker names, or using de-identification techniques, such as facial and body blurring or ghosting, can be an effective and straightforward method of enhancing data privacy. This solution is often easily implementable.



Data
minimisation

Ensure data minimisation. With technological progress and the continuous miniaturisation of sensors, there is a growing temptation to incorporate multiple sensors into hardware devices such as wearables and integrate their measurements. However, it is crucial to exercise caution in this context to prevent the collection of data that may not be relevant for safety and health purposes.



Compliance

Ensuring that smart digital systems adhere to relevant data protection laws and regulations, such as the General Data Protection Regulation⁸ in Europe, can also help enhance data privacy and clarify potential questions around the collection and use of data.



Storage and
cybersecurity

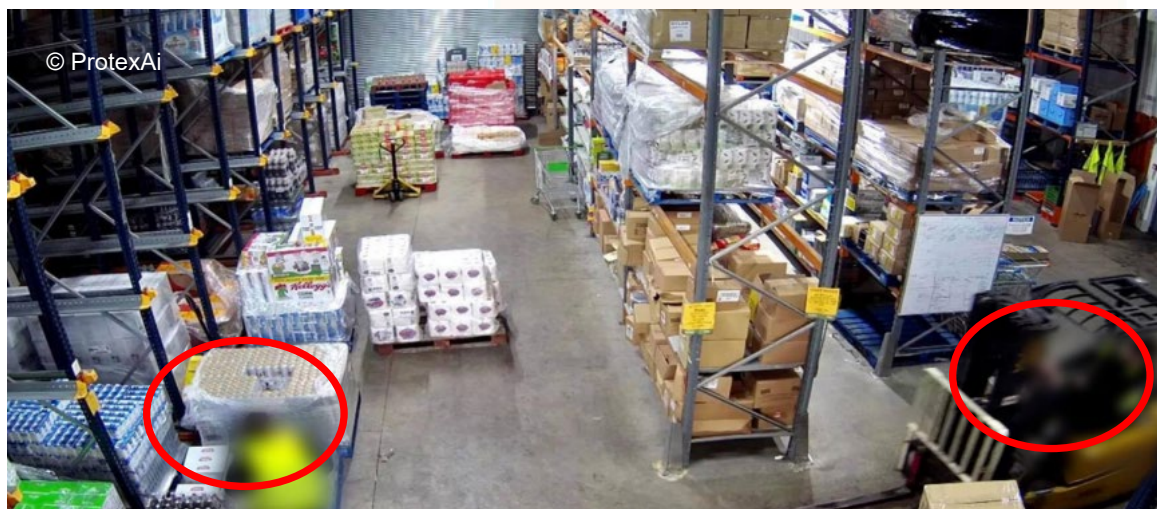
Storing the data in secure servers and using strong cybersecurity measures can help reduce the risk of data breaches that might compromise workers' personal data if they are not anonymous.

⁷ In EU-OSHA's publications, the terms "designer", "implementer" and "system user" are used. These publications were prepared before the AI Act ([Regulation \(EU\) 2024/1689](https://eur-lex.europa.eu/eli/reg/2024/1689/oj)) was adopted. With the AI Act new terms such as "provider" and "deployer" have also been introduced.

⁸ European Commission. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434>

Depending on the specific smart monitoring system, there are also other ways of ensuring privacy by design. For example, a developer from Ireland has developed AI software analysing video footage to detect unsafe events at the workplace. This AI software embeds, by its design, worker 'de-identification techniques', such as facial and body blurring or ghosting (see Figure 2).⁹ As shown earlier, most developers can also decide to anonymise data and/or use workers' data in an aggregate manner, which often provides the most valuable insights for employers.

Figure 2: Embedding privacy by design in camera-based smart monitoring systems



Privacy by choice

On some occasions, integrating privacy by design might not be the most suitable approach. For example, for remote or high-risk environments such as mines, it is important for smart monitoring systems to have the capability to track workers, especially in the event of a rescue operation. Likewise, on occasions where the smart monitoring systems aim to monitor the risks of musculoskeletal disorders (MSDs) and offer personalised feedback to workers — according to, among other factors, their age, height, weight and other characteristics — having access to personal or sensitive information is important. In these cases, data privacy can still be preserved, through different options. Some practical ways to achieve this are set out in Figure 3.

Figure 3: Privacy by choice¹⁰



Determining
access to data

Restricting data access to designated persons can be an effective way of making sure that the data collected are used exclusively for safety and health purposes.

⁹ See presentation material at euosha-events.eu (2023). 'High-level Workshop Smart Monitoring Systems'. <https://www.euosha-events.eu/smart-digital-systems/>

¹⁰ Unless otherwise stated, the information in this figure is taken from euosha-events.eu (2023). 'High-level Workshop Smart Monitoring Systems', presentation material. <https://www.euosha-events.eu/smart-digital-systems/>



A Swedish mining company, using a smart monitoring system with geolocation functions, stores all of the workers' data on a hard drive that is owned and exclusively accessed by the workers' union. In extraordinary circumstances, such as accidents, geolocation data are shared with rescue teams to improve the time of the rescue operations for individual workers.



A developer based in France, producing smart insoles equipped with 'worker-down' and voluntary alert features for remote workers, triggers the insole's geolocation system exclusively in the event of emergencies. In the absence of emergencies, the geolocation system is turned off.



A United Kingdom-based developer, producing a wearable device monitoring the risks of MSDs, gives direct feedback to workers through beeps and buzzes. The wearable device is linked to a companion app where workers can view their individual results and engage with micro-learning tutorials. At the same time, the same information is anonymised and sent in an aggregate form to OSH professionals, who can use it to compare risks across workers, groups and sites.



A Dutch developer, piloting software that allows workers to self-report feelings of stress, grants access to this information solely to OSH professionals, such as psychologists, who are not affiliated with the human resources departments of the workers' places of work.

Conclusions

Workers tend to have a positive attitude towards using smart digital systems, provided that any concerns regarding their use are adequately addressed and clarified.¹¹

As regards data privacy, some worker concerns can be addressed at the design stage of a smart monitoring system. This can be achieved by anonymising data, minimising the collection of unnecessary data, and incorporating features such as facial and body blurring or ghosting, as seen in camera systems, among other measures.

When such measures are not the most suitable option, determining data ownership and access can be a practical solution to addressing data-related concerns. For example, restricting data access to workers and OSH professionals or physicians, as well as opting out from certain options of the smart digital systems, such as the sharing of geolocation data when there are no emergencies, can be effective ways of addressing concerns about potential misuse of these systems. Equally, anonymising and aggregating data can serve the same purpose.

To this end, **consultations between workers' organisations and their members**, or their representatives, can be a key success factor for the effective implementation of smart monitoring systems in the workplace. This can help employers and workers find mutual solutions around the use of data from smart monitoring systems and clarify any concerns raised by workers.

¹¹ EU-OSHA – European Agency for Safety and Health at Work, *Smart digital monitoring systems for occupational safety and health: workplace resources for design, implementation and use*, 2023. Available at: <https://osha.europa.eu/en/publications/smart-digital-monitoring-systems-occupational-safety-and-health-workplace-resources-design-implementation-and-use>

Authors: Kyrillos Spyridopoulos, Andrea Broughton (Ecorys).

Project management: Annick Starren, Ioannis Anyfantis - European Agency for Safety and Health at Work (EU-OSHA).

This policy brief was commissioned by the European Agency for Safety and Health at Work (EU-OSHA). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect the views of EU-OSHA.

Neither the European Agency for Safety and Health at Work nor any person acting on behalf of the Agency is responsible for the use that might be made of the above information.

© European Agency for Safety and Health at Work, 2024

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the copyright of the European Agency for Safety and Health at Work, permission must be sought directly from the copyright holders.