Be smart,
stay safe together –
Innovative products and
workplaces

CIOP PIB

# Personal data protection and cybersecurity issues with regard to the design and use of smart PPE

**Daniel Podgórski & Grzegorz Owczarek**

Central Institute for Labour Protection - National Research Institute

Warsaw, Poland

6th EUROSHNET **Conference on standardization, testing and certification** in the field of occupational safety and health
12-14 June 2019, Dresden, Germany

# New functions of Smart PPE

**Sensing:**

- Monitoring of environmental hazards and risks
- User localisation (e.g. in relations to danger zones)
- Monitoring of physiological parameters

**Reacting to control risks:**

- Self-adjusting of protective properties
- Providing warnings and work instructions
- Activation of external (engineering) risk controls

**Supporting PPE operation:**

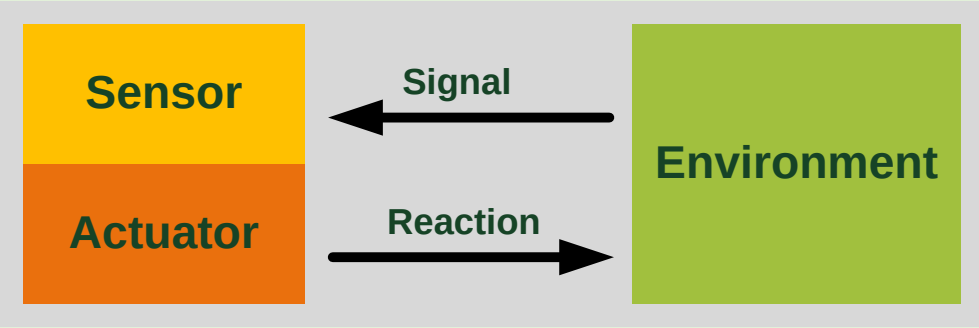
- End-of-service-life indication
- Energy harvesting and storage

# Three levels of smart PPE complexity (intelligence)

## Level 1

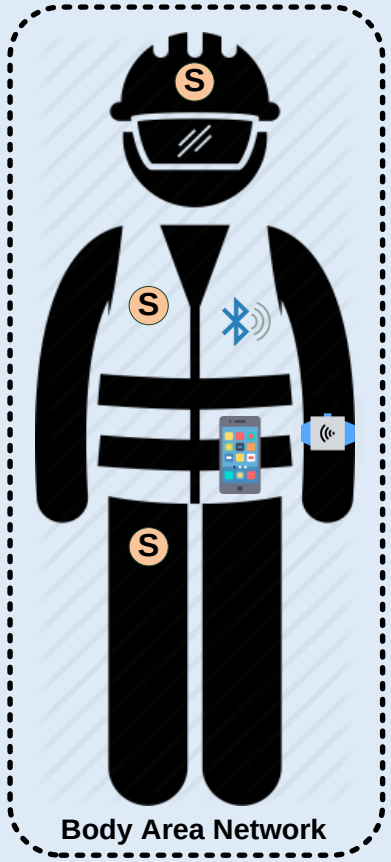
PPE solutions based on **smart textiles**, e.g. Phase-Change Materials (PCM), Shape Memory Alloys or simple electronics:

- capable to control single risk factors
- **no ICT modules - no data** generation and processing



# Three levels of smart PPE complexity (intelligence)

## Level 2




Detect hazards & evaluate risks

Communicate risks to worker

Control risks & monitor PPE functions

**Autonomous smart PPE** systems with built-in sensors, actuators and **ICT modules**:

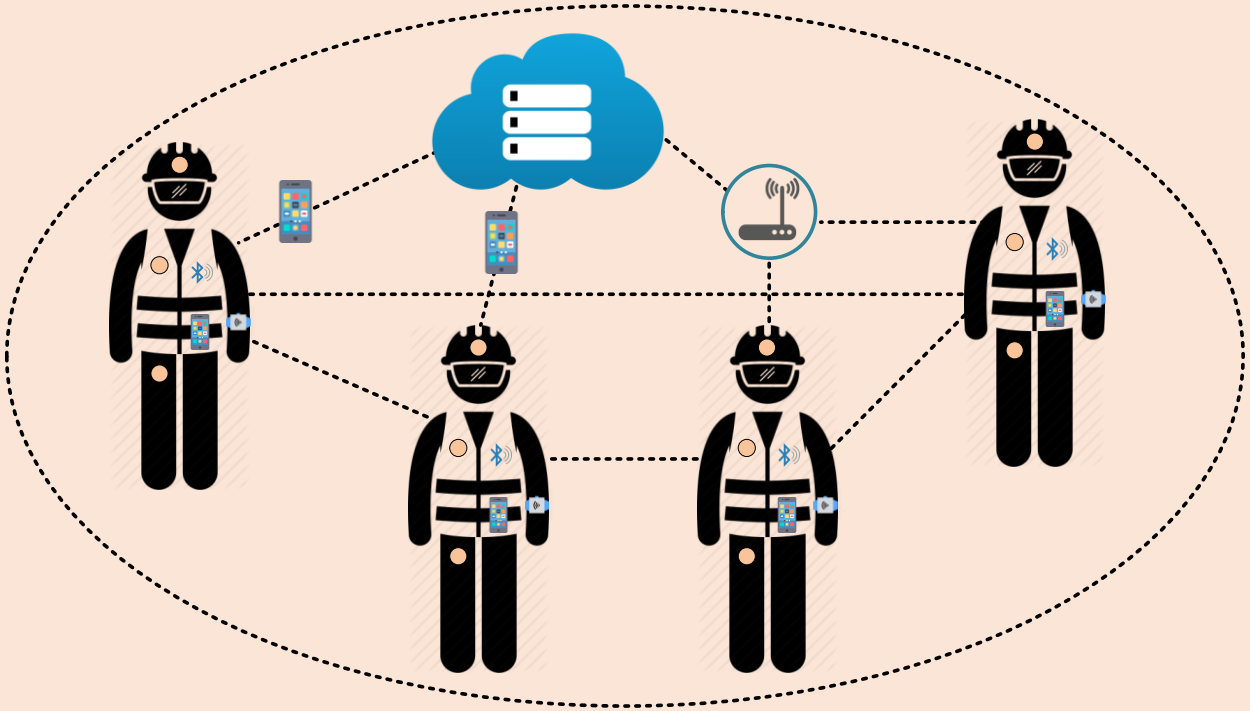
- capable to control several risk factors
- **data generation and processing**, but data transmission rather limited to user's Body Area Network

# Three levels of smart PPE complexity (intelligence)

## Level 3

**Networked PPE systems** with built-in sensors and ICT modules, connected with external **DATA processing** servers (e.g. cloud-based or local) and with the PPE systems of other users

- capable to control multiple risk factors
- risk control functions may cover many users at the same time
- generation and processing of **large amounts of data**
- advanced **data analytics** can be applied for **OSH management functions**



# Examples of IoT-based Smart PPE systems (level 3)

### Corvex Connected Safety and HexArmor

Monitoring:

- proximity to high-risk zones
- proper PPE usage
- real-time incident reporting
- workers' involvement in safety

### Cybercom Connected Helmet

Monitoring:

- workers' localisation, including in hight
- proper usage of the helmet
- external temperature

### IBM Maximo Worker Insights

Gathers data from wearables that monitor:

- high temperature
- heart rate (fatigue)
- fall detection
- proximity to hazards

Sources:

- www.hexarmor.com/posts/hexarmor-partners-with-first-worker-powered-iot-safety-platform
- www.cybercom.com/globalassets/poland/iot/ulotki/connected_helmet_product-description_en.pdf
- www.ibm.com/us-en/marketplace/iot-safer-workplace/details
- play.google.com/store/apps/details?id=com.ibm.iot.workerinsights

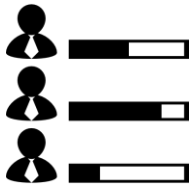
# Data that can be measured and collected by smart PPE

## Health status (medical) data:

- heart rate (HR)
- body temperature
- blood pressure
- oxygen consumption
- galvanic skin response (GSR)
- stress hormones, etc.

## Location and interaction:

- user location in relation to danger zones
- time spent in individual places (rooms)
- behaviours, contacts with other workers, etc.



## Worker performance

- time spent on performing individual tasks
- duration of rest breaks
- workers' cognitive patterns, etc.

# GDPR: General Data Protection Regulation

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

- Data concerning health belongs to data of special category
- Health data means data related to the physical or mental health of a person which reveal information about his or her health status
- Processing of special categories of personal data (including health data) shall be prohibited

# Processing health data under GDPR

**Processing of data concerning health is allowed if:**

- the data subject has given **explicit consent to the data processing**
- **processing is necessary** for the purposes of:
  - preventive or occupational medicine,
  - assessment of the working capacity of the employee, …

**Processing of health data collected by a smart PPE system may be permitted, but only under special conditions.**

# Profiling under GDPR

**Profiling** - automated processing of personal data to evaluate certain personal aspects, in particular to analyse or predict aspects concerning performance at work, economic situation, health, personal preferences, reliability, behaviour, location or movements.

- **All personal data** collected at the workplace **can be used for profiling**
- **The data subject shall have the right not to be subject to a decision based on profiling** which significantly affects him or her
- **Profiling may be allowed** if the data subject has given **explicit consent**

# But how to implement these provisions in practice?

## Some basic rules stemming from GDPR

**Data minimalisation:** Collect only what you need

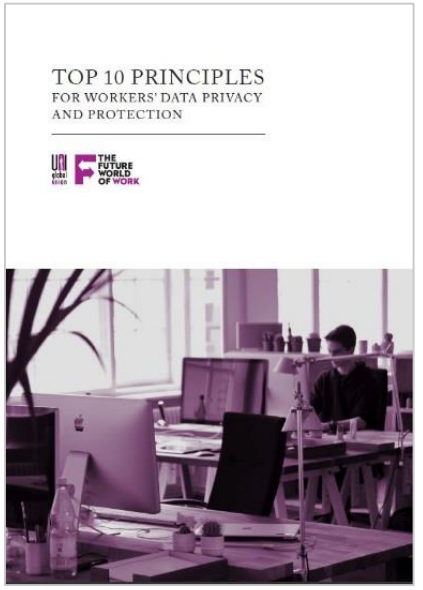
**Pseudonymisation:** Separate personal data from the rest

**Transparency:** Explain your processing purpose

**Authorisation:** Granting access to authorised persons

**Informed consent:** Freely given, specific and informed

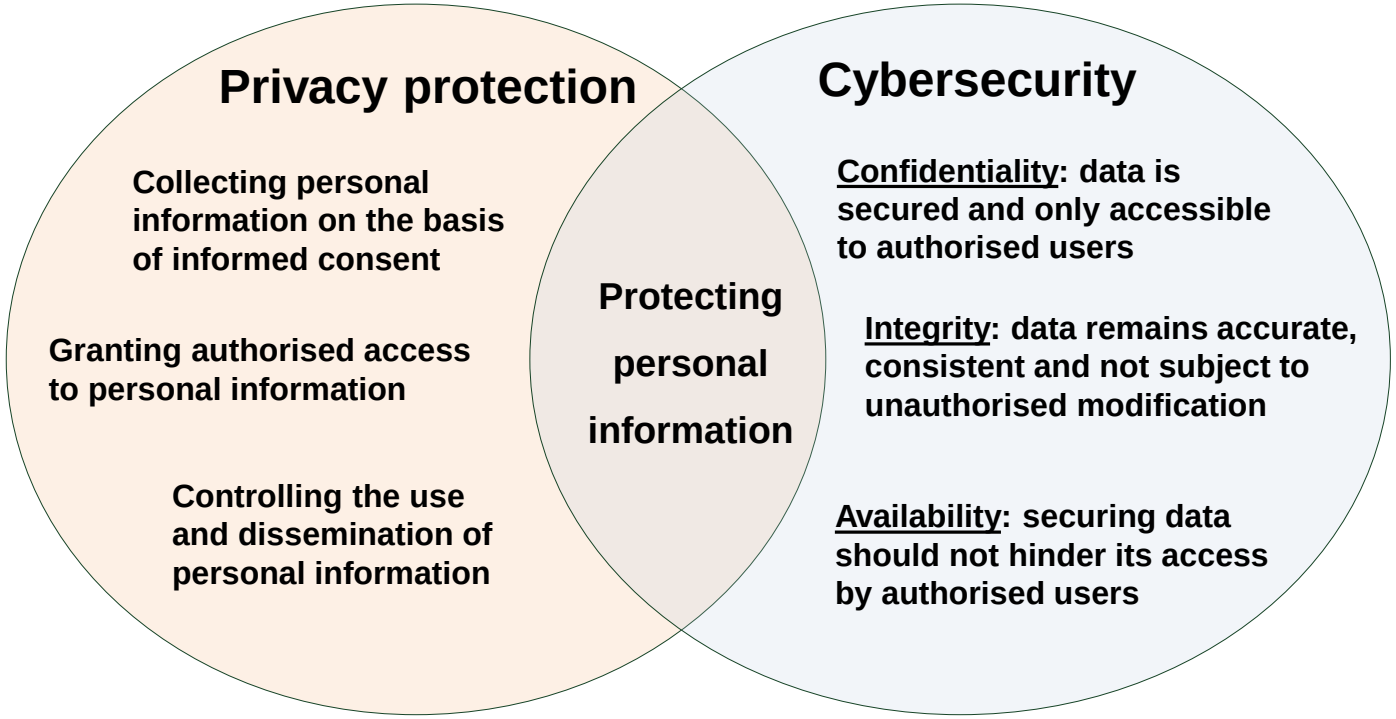
**Monitoring:** Continuously check data collection process


UNI Global Union

# Privacy protection vs. Cybersecurity

- **Privacy protection** consists of awareness of privacy risks, individual control over the collection and processing of personal data, and awareness and control of use and dissemination of personal information
- **Cybersecurity** means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats



# Example scenarios of cyber risks

- A cyberattack may disable functions of a health monitoring system of lone workers and may lead to leaving them unsupported in hazardous conditions.

  **Operational risk:** disrupting control and/or communication functions

- Stealing workers' health information by a hacker to use it for blackmailing and extortion or to sell for marketing purposes (e.g. advertising medical products).

  **Informational risk**: the loss, unauthorised access to, destruction, or other unintended use of electronic information

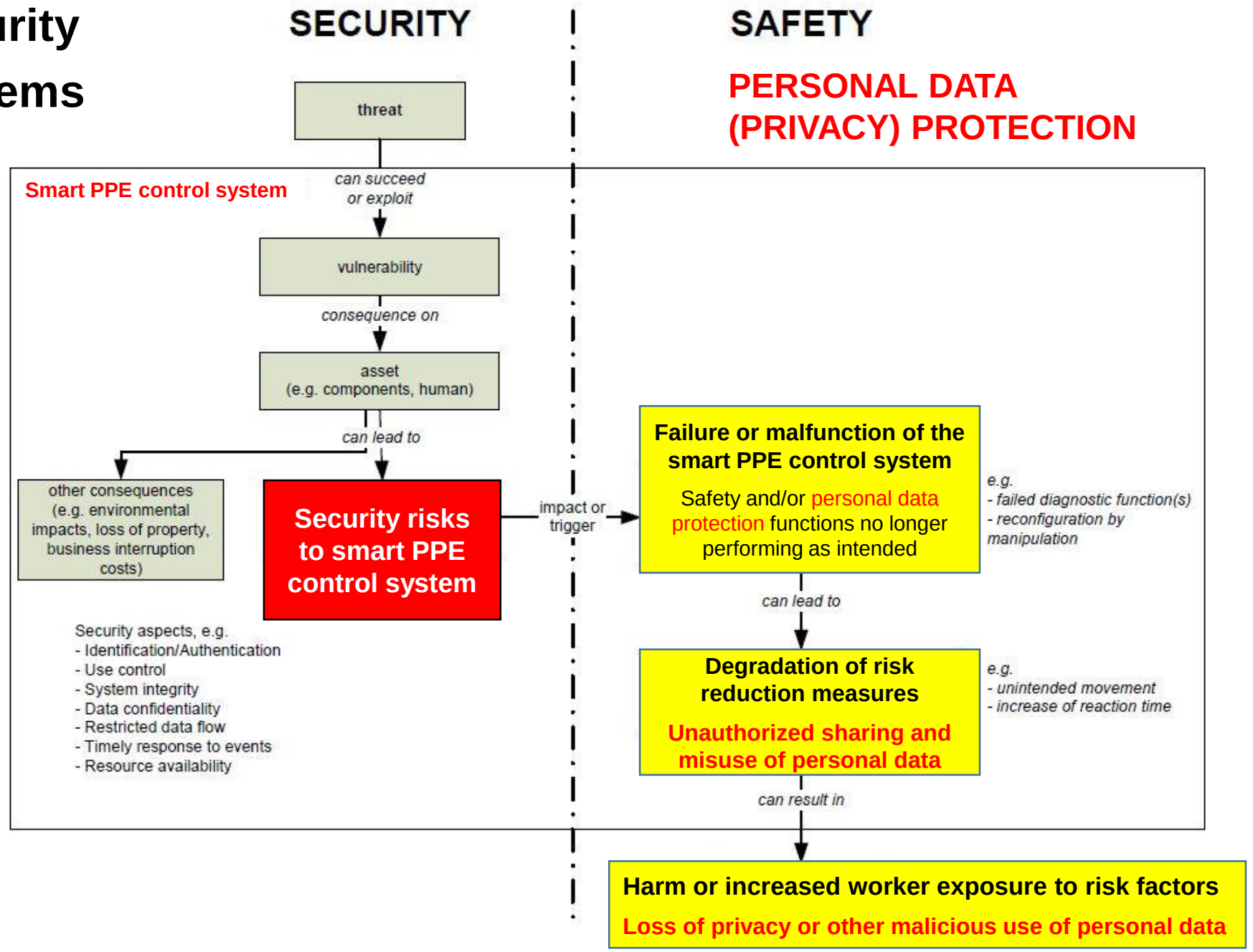
- Hacking Augmented Reality devices (smart glasses) that will allow to take control of the system and display false instructions to the user. These may result in incorrect actions leading to a damage to machinery or entire system.

  **Physical risk:** physical damage or unexpected physical events caused by actions in the cyber domain

(Categorisation of cyber risks adapted from Barbour SHP, 2017)

# The impact of cybersecurity risks on smart PPE systems

## Potential consequences for safety and health and personal data protection




Adapted from IEC TR 63074 ED1 (2018): *Security aspects related to functional safety of safety-related control systems*

# Some general recommendations for IoT cybersecurity

- Edge/Fog computing solutions to limit cloud-based data processing
- Cloud services which ensure the highest level of data security
- User authentication and authorization (incl. biometric techniques), i.e. verifying the identity of a user (but ensuring anonymity) or a device as a prerequisite for granting the access to system functions
- Anti-virus tools and malware testing to prevent, detect, and remove any malicious software introduced into the system
- Efficient security protocols and encrypting algorithms, particularly in case of transmitting and storage of personal data

# EU regulation on cybersecurity

- **Cybersecurity Act** - **Regulation (EU) 2019/881** of the European Parliament and of the Council of **17 April 2019** on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) no. 526/2013
- **Published on 7 June 2019, will enter into force 20 days after publishing** (art. 58, 60, 61, 63, 64 i 65 will enter into force in June 2021)
- Reinforces and strengthens ENISA
- Establishes the first **EU-wide cybersecurity certification framework**

# EU cybersecurity certification framework

- **Establishement of EU cybersecurity certification schemes** to attest that the ICT products, ICT services and ICT processes comply with specified cybersecurity requirements
- **One or more assurance levels** for ICT products, services and processes could be established: **basic, substantial or high**
- The **assurance level should be relevant to the level of cyber risk** associated with the intended use of the ICT product, service or process
- **Smart PPE systems** may become **subject to EU cybersecurity certification** if:
  - they become the target of cyberattacks
  - there will be sufficient market demand

# Standardisation

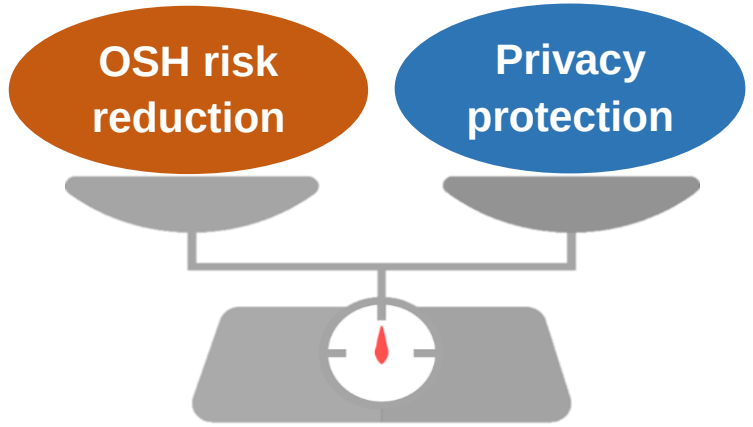
## Cybersecurity

- **CEN/CENELEC JTC 13** Cybersecurity and Data Protection (cybersecurity and data protection covering all aspects of the information society)
- **ETSI** Technical Committee Cyber Security (CYBER)
- **UL 2900** standards on Software Cybersecurity for Network-Connectable Products
- **NISTIR 8196**: Security Analysis of First Responder Mobile and Wearable Devices (draft), National Institute of Standards and Technology (NIST), USA, 2018

## Smart PPE, smart textiles and wearables

- **CEN TC 162** Protective clothing including hand and arm protection and lifejackets (work items related to the EC mandate M553, e.g. draft Technical Report)
- **CEN/TC 248** Textiles and textile products, WG 31 Smart Textiles
- **IEC TC 124** Wearable electronic devices and technologies

# Summary




- Smart PPE systems have a high potential to be used in a broader OSH management context allowing for advanced data analytics and actionable insights
- Succesful implementation of smart PPE requires a careful balance between OSH risk reduction and protection of workers' privacy
- Medical data measured in the workplace belong to workers and should be protected
- ICT-based smart PPE systems should be protected against cyberattacks
- Meeting GDPR and cybersecurity requirements may be crucial for the future uptake of smart PPE technologies by the industry and the market
- Should EU future cybersecurity certification cover smart PPE systems?

# Thank you for your attention

The presentation is based on the results of R&D projects carried out at CIOP-PIB within the National programme ***Improvement of safety and working conditions***, financed by the Polish Ministry of Family, Labour and Social Policy and the Ministry of Science and Higher Education (2014- 2019).

The content particularly refers to the **project 3.G.05**

## *Guidelines for the protection of personal data and cybersecurity in smart personal protective equipment systems*

carried out by **Dr. Grzegorz Owczarek**, CIOP-PIB, Department of Personal Protective Equipment, with the participation of **Dr. Artur Hłobaż**, University of Łódź, Faculty of Physics and Applied Informatics.