Data management

There is a need to develop a plan for the management of data collected from low-cost sensors. This guidance sheet provides further information on the points to consider when developing your plan.

Management of low-cost sensor data is subject to the same data security, processing, retention and privacy considerations as any business data. Your organisation should have policies and procedures already in place which governs this data.

Security, Privacy and Legal considerations

- **Regulatory compliance:** Identify relevant national/regional legislative requirements regarding data collection, processing, storage, privacy and sharing and ensure compliance with these. Low-cost sensors which are used for personal monitoring may also be subject to consideration as sensitive data under the General Data Protection Regulation (GDPR) or other local data privacy laws.
- **Consent process:** Depending on country specific requirements, informed consent may be required from workers concerning the wearing of personal low-cost sensor devices. Your organisation should have policies and procedures concerning the consenting process.
- **Data anonymization/pseudonymisation:** Define data that is sensitive and put policies in place to either anonymize data (where the data is processed so that it makes it impossible to identify individuals from them) or pseudonymise the data (which makes the personal data unidentifiable to a specific person without any extra information). This to protect workers identities and ensure compliance with local data privacy laws.
- **Data ownership and sharing:** Define who owns the low-cost sensor data and under what conditions it can be shared with third parties (and who these may be). Define data sharing agreements.
- **Data access:** Define who is authorised to access the data and what they can use it for.
- **Data encryption:** Define if there is a need to encrypt data, particularly important if dealing with personal, sensitive information.

Data Storage, Back-up, and Retention considerations

- Low-cost sensor companies may provide some sort of cloud-based storage and management of data. It is important to check with the company where the data is stored, what legislative requirements are in place in that jurisdiction, who has access to the data, whether data can be traced back to its originator and how long it is stored for. Ensure that the responses you obtain meet your and your company needs, as well as fulfil the security, privacy and legal considerations mentioned previously. You should also check whether it is possible to download and store the data locally.
- If you are downloading and storing your data through your own internal systems, ensure that the following considerations are addressed.
    - Local storage: Define where the data will be stored locally (e.g., memory card, company sever) and who is responsible for its storage.

- Data retention policies: Define how long data should be stored (which will also depend on the intended purpose of the data), who has access to the data and who is responsible for its deletion.
- Data backup: Define procedures for the back-up of the data to prevent loss.

Ultimately, your organisation should decide what is the most suitable data storage solution, which may be local, cloud-based, or a combination of the two, for your requirements.