KU LEUVEN
HIVA
RESEARCH INSTITUTE FOR
WORK AND SOCIETY

TURNING ETHICAL CHALLENGES INTO DESIGN REQUIREMENTS

Insights from literature and expert interviews on operator well-being monitoring

REPORT

Michiel Bal & Ezra Dessers

July 2025

TURNING ETHICAL CHALLENGES INTO DESIGN REQUIREMENTS

Insights from literature and expert interviews on operator well-being monitoring

Michiel Bal & Ezra Dessers

This research is part of the Flanders Make SBO project 'Wellficiency'

Published by

KU Leuven
HIVA – RESEARCH INSTITUTE FOR WORK AND SOCIETY
Parkstraat 47 bus 5300, 3000 LEUVEN, Belgium
hiva@kuleuven.be
https://hiva.kuleuven.be

© 2025 HIVA-KU Leuven

Bal, M., & Dessers, E. (2025) Turning ethical challenges into design requirements. Insights from literature and expert interviews on operator well-being monitoring. HIVA - KU Leuven.

No part of this book may be reproduced in any form, by mimeograph, film or any other means, without permission in writing from the publisher.

Abstract

This report explores the ethical and privacy dimensions of continuous employee well-being monitoring in industrial settings, as developed within the WellFiciency project. The project aims to create a technology-supported methodology that integrates subjective and sensor data to build a digital twin of the operator, feeding into well-being dashboards and a well-being-aware allocation and scheduling tool. Recognising the potential ethical challenges, the report combines insights from a comprehensive literature review and 25 stakeholder interviews, including practitioners, researchers, social partners, and legal experts. The analysis addresses issues related to data governance, transparency, participation, and contextual variability across sectors and countries. Based on these findings, the report formulates a structured set of design requirements to guide the responsible development and implementation of the WellFiciency methodology. These requirements aim to balance technological innovation with ethical integrity, supporting adoption in real-world industrial environments.

Management summary

This report draws on a comprehensive literature review and expert interviews to examine the ethical and privacy dimensions of measuring and processing operator well-being data. This management summary provides an outline of the design requirements identified in our study. It should be noted that this overview does not include the level of detail needed to operationalise these requirements in practice. We group the requirements according to five guiding topics.

Design requirements related to legislation: ensuring legal soundness of the methodology

- Legitimacy:
  - the methodology must align with the prevention principle, recognising well-being as a collective concern within the organisation;
  - personal data must be collected on a voluntary basis, processed fairly, and used for clearly defined, legitimate purposes.

- Proportionality: data collection must be purposeful, necessary, and limited to what is strictly required for the intended objectives.

- Transparency: the organisation must implement a transparent policy regarding the collection, use, and management of operator well-being data, ensuring clarity on related practices and developments.

- Confidentiality: all individuals or entities with access to personal data must be formally bound by confidentiality obligations.

- Accessibility: each individual must have access to their own well-being data in an understandable and usable format.

- Ethical awareness:
  - project partners must distinguish between what is legally permitted and what is ethically responsible;
  - legal frameworks should be treated as setting the minimum standard; the methodology must strive to meet higher ethical benchmarks.

Design requirements related to deontology: ensuring ethical development of the methodology

- Participation and involvement: the methodology must ensure meaningful participation of stakeholders throughout its development, recognising that:
  - greater depth of participation (e.g. active engagement in design decisions) increases acceptability and adoptability;
  - broader inclusion of diverse stakeholder groups enhances legitimacy and support;
  - early-stage involvement fosters trust and ownership;
  - communication must be timely, transparent, and tailored to the concerns and language of specific stakeholder groups.

- Data literacy and data awareness:
  - stakeholders must be adequately informed about relevant legal frameworks governing data use, enhancing their data literacy;
  - stakeholders must be made aware of the potential consequences and implications of data collection and use, fostering data awareness and informed consent.

Design requirements related to consequentialism: ensuring the methodology reaches its intended goals

- Evaluation of interventions: the methodology must account for the mixed reception of interventions such as task rotation, and include mechanisms to evaluate their actual impact on well-being.

- Empowerment versus constraint: the use of well-being data must be designed to empower workers rather than constrain their autonomy; this balance must be continuously monitored and adjusted as needed.

- Anticipation of normalisation effects: the risk that data collection and feedback lead to implicit norms or pressures on behaviour (data-imposed normalisation) must be anticipated, made explicit, and addressed in follow-up measures.

- Prevention of data-facilitated harm: potential negative effects of well-being data use (e.g. stigmatisation, exclusion, increased stress) must be proactively identified and mitigated.

- Clarity on responsibilities and accountabilities: roles, responsibilities, and lines of accountability related to the collection, interpretation, and use of well-being data must be clearly defined and openly discussed.

- Transparency on actionable outcomes: expectations regarding how the data will lead to action must be made transparent to all stakeholders, including the limitations of what can or will be done.

Design requirements related to methodology: ensuring accurate measurement of operator well-being

- Validity: the methodology must critically assess whether the well-being indicators and data sources accurately reflect the actual experiences of operators, acknowledging the limits of datafication.

- Reliability: the methodology must ensure consistency in measurement over time and across contexts, while remaining vigilant for risks of manipulation or behavioural modification due to monitoring.

- Interpretability: the data must be interpretable for both researchers and organisational stakeholders, with clear links between indicators and practical meaning.

- Reactivity: the methodology must account for the fact that sharing or visualising well-being data may itself influence the well-being of operators, and manage this reactivity carefully.

- Aggregation: conditions for aggregating individual well-being data must be made explicit, including how aggregation may be affected by participation bias or limited data coverage.

- Technological feasibility and intrusiveness: the selected technologies must be feasible for implementation in real industrial settings, and their intrusiveness must be assessed and minimised to protect user comfort and trust.

Design requirements related to organisational fit: ensuring alignment with the organisational context

- Alignment with collective concern: The methodology must reinforce the notion of well-being as a shared, collective concern, avoiding an individualised or solely self-responsibilising approach.

- Integration with existing initiatives:
  - existing well-being initiatives, including their scope, reach, and limitations, must be identified and acknowledged.
  - the new technological approach should complement and strengthen existing practices, not displace or undermine them.

- Recognition of organisational dynamics: the role of the union must be respected, and the underlying agendas of both employers and employees should be made visible and taken into account in the development and implementation of the methodology.

- Clarity on participation consequences: the expected outcomes and potential consequences of employee participation in the methodology must be clearly communicated, including how input may influence organisational decision making.

It should be noted that different key stakeholder groups involved in the development and regulation of well-being monitoring technologies typically have specific concerns. Workers express concerns about surveillance, lack of transparency, and exclusion from decision making. Employers are challenged to balance data use with trust and responsibility. Unions and works councils advocate for worker rights. External experts, including prevention advisors and psychologists, stress the need for privacy-conscious and participatory approaches. Regulatory bodies ensure legal compliance, but gaps remain in adapting to fast-evolving technologies. The findings highlight the importance of inclusive, transparent, and ethically grounded design choices when developing and implementing well-being monitoring systems.

Contents

ABSTRACT **2**

MANAGEMENT SUMMARY **3**

LIST OF TABLES **8**

INTRODUCTION **9**

PART 1 LITERATURE REVIEW **10**

INTRODUCTION **11**

1 Ethical opportunities 13
1.1 User empowerment 13
1.2 Contribution to health and well-being 13
1.3 Community building and solidarity 14

2 Ethical challenges 15
2.1 Enforced social harm 15
2.2 Internalised responsibility 16
2.3 Constrained autonomy 16
2.4 Data-facilitated harm 17
2.5 Datafied or reified employees 17
2.6 Data validity and reliability 18
2.7 Flawed interpretability of well-being data 19
2.8 Reduced self-image 19
2.9 Lack of transparency 20
2.10 Regulative framework 20
2.11 Ownership, control and commodification of data 21
2.12 Privacy 22
2.13 Surveillance 23

3 Conclusion 24

REFERENCES **25**

PART 2 INTERVIEWS **28**

INTRODUCTION **29**

1 Method 30
2 Results 32
2.1 Ethical considerations in the process of developing and implementing the assessment 32
2.2 Ethical considerations on the outcomes resulting from measurement 38

2.3	Ethics and the balance of unitarist and pluralist interests at work	51
2.4	Legal framework(s)	57
2.5	Legislation: different types at different levels	58
2.6	Methodological challenges	66
2.7	Ethics in relation to various contextual characteristics	74
2.8	Relevant parties	78
3	Conclusion	83
PART 3 DESIGN REQUIREMENTS		**84**
INTRODUCTION		**85**
1	Process ethics	88
1.1	Participation	88
1.2	Social dialogue	89
1.3	Data literacy and data awareness	89
1.4	Communication	90
2	Outcome ethics	91
2.1	Task rotation	91
2.2	User empowerment?	91
2.3	Constrained autonomy?	92
2.4	Data-imposed normalisation	92
2.5	Data-facilitated harm	92
2.6	Responsibilities and accountabilities	93
2.7	Expectations and actionality	93
3	Legal principles	94
3.1	The principle of legitimacy	94
3.2	The principle of proportionality	94
3.3	The principle of access	96
4	Methodological requirements	97
4.1	Validity	97
4.2	Datafication	97
4.3	Reliability	98
4.4	Manipulation and modification	98
4.5	Data interpretability	98
4.6	Data reactivity	99
4.7	Data inference	99
4.8	Data aggregation and participation bias	99
4.9	Technological feasibility and intrusiveness	100
General conclusion		101

List of tables

TABLE 2.1 Table of Interviewees 31

Introduction

The goal of the WellFiciency project is to develop a technology-supported methodology to measure employee well-being of industry operators continuously, combining subjective and sensor data to build a digital twin of the operator. This data feeds into well-being dashboards and a well-being-aware allocation and scheduling tool. Beyond the technical and methodological complexities, the approach also raises significant ethical and privacy concerns. Addressing these challenges is essential for ensuring the methodology's practical adoption in industrial settings. This report draws on a comprehensive literature review and expert interviews to examine the ethical and privacy dimensions of measuring and processing operator well-being data. Based on these insights, we propose a structured set of design requirements to guide the development of the WellFiciency methodology.

PART 1
LITERATURE REVIEW

Introduction

This first part studies the current state of the art on the ethical debate with regards to employee well-being (EW) assessment tools, that include a.o. people analytics at work, organisation safety and health monitoring technologies, self-tracking at work, mHealth at work, the quantified self at work, and related developments. Before doing so, we shortly define ethics and moral behaviour. *Ethics* are the philosophical discipline that deals with values norms, rights, duties, goods and virtues (Wieczorek *et al.*, 2023). More particularly, ethics are concerned with benefiting others, in particular and universally, and with improving the world within which each and all of the members of society participate. There is an essential reciprocity to ethical thought and moral behaviour that is found universally in the golden rule of ethics: '*do to others what you would have them do to you, and its negative: do not do to others that which you would not have them do to you*' (McAleenan *et al.*, 2018). Consequently, ethical aspects of any given subject, in our case to collecting, storing, analysing and disseminating EW data, are the features one may raise questions about regarding norms, rights, values, goods and virtues. Among the broader ethical questions, particular attention will be drawn in this report to the moral, privacy-related and legal framework surrounding data collection, storage, analysis and dissemination. For the literature overview, we will build on academic and grey literature on the topic of well-being measurements.

As the following sections will show, ethics research in the area of measuring EW at work by means of new, emerging wearable technologies is still at an early stage. Optimistic and technocentric perspectives are still dominating the discourse. Although diverse stakeholder inclusion has been promoted in research, just like transparency, and the fair and proportionate use of data, there is still a long way to go to obtain a culture that is systematically fostering ethical practice, and delivering benefits for employees. To a great extent current work on data collecting technologies draws on traditional principles of human resources management (HRM). In that sense, the availability of personnel data may cause a seismic shift in the power of organisations and their leaders to understand, and more particularly, strategically optimise and plan their workforce. Much of the literature discusses the benefits the technology brings to the workplace from a managerial perspective and generally assumes that such benefits will automatically benefit the workforce.

However, a major flaw in much of the literature is that it fails to ask workers what they truly think is needed. It fails to consider the repercussions of such monitoring technologies on employees, simply by just bypassing the ones who are (to be) using these technologies. This is remarkable, since people analytics, self-tracking and related developments are becoming increasingly topic of discussion in projects, that thus highly depend on ethical requirements such as privacy and acceptability. Peterson *et al.* (2018), for instance, reported that in a survey of around sixty companies four out of five respondents reported that workforce analytics were either 'sometimes' or 'often' jeopardised by data ethics or privacy concerns.

In addition, much of the literature assumes that ready-made monitoring technologies just will work out as intended, and benefit employees in purposed ways (i.e. technological solutionism). Consultation and discussions on the technologies are still rare phenomena. Moreover, the basic question of what can be done better to make jobs healthier and safer is largely missing in this domain. Ultimately, despite the significant risks of the technology-focused and imposed solutions (Marler & Boudreau, 2017; Tursunbayeva *et al.*, 2018, 2021; Wieczorek *et al.*, 2023) that mostly relate to

privacy and autonomy, there has been a near absence of ethical considerations in the corpus of academic grey and online literature.

We begin by outlining three ethical opportunities, followed by an overview of ten ethical challenges, including shortcomings and drawbacks.

1 ETHICAL OPPORTUNITIES

The ethical affordances commonly associated with EW assessment tools are in this section grouped into three categories: (1) user empowerment, (2) promotion of health and well-being, and (3) community building and solidarity. The premise of this section is that EW assessment tools have the potential to improve EW. By visualising EW, these instruments tend to *augment* employees' knowledge about their own well-being, create more awareness for the topic, and at least give them data as handhelds based on which they could act.

1.1 User empowerment

The positive effects EW self-assessment tools can have on user empowerment and well-being are in the first place well-mentioned in the literature. Interestingly, the empowering potential would be the greatest when users can modify their own devices onto their own needs, and if they can amend personal parameters that are mostly in line with their individual needs (Sharon, 2017; Sharon & Zandbergen, 2017). Thus, user autonomy is enhanced through active engagement with, for example, wearable technology, rather than passive acceptance of the software platform (Bal *et al.*, 2023; Wieczorek *et al.*, 2023).

Others emphasise the extension of users' decision making capabilities (Danaher, 2018; Duus *et al.*, 2018). Regarding the decision making capabilities, we also refer to the job autonomy. Enhanced decision making capabilities may in turn contribute to end-users' self-confidence helping them to deal with anxiety, or feelings of inadequacy.

Till (2019) additionally claims the deployment of wearables in the workplace fosters employee well-being, while simultaneously increasing their productivity, and thus also prove benefits for the employers. In contrast, Schulz (2016) analyses tracking and EW self-assessment tools from a Marxist perspective which considers labour as alienating the workers, and this author is critical regarding the deployment of the tools that would foremost empower the employer at the expense of the employee. It should be noted that some authors tend to make vague or unsubstantiated claims about empowerment and well-being, merely echoing the promises of self-tracking promoted by marketing advocates '.

1.2 Contribution to health and well-being

In the second place, the relatively optimistic EW self-assessment literature mentions that the tools may contribute to good health. Requirement is that users should be enabled to improve their own health by monitoring factors relevant to their condition (Ajana, 2017; Gabriels & Moerenhout, 2018). Wieczorek *et al.* (2023) notice this can be particularly interesting and relevant for individuals living with chronic illnesses that already require them to keep track of significant number of factors. Translated to the context of the workplace, and more specifically to the WellFiciency-project, it may be valuable for operators to keep track of their physical and mental well-being, as operators are

often confronted with heavy load, and sometimes unfavourable work conditions. Enhanced information by means of a data overview may then be a necessary stepping stone to alter the conditions. An every day, continuous overview of employee well-being based on objective physiological and subjective questionnaire-based data may not only reduce the reliance on professional care, and reduce other healthcare costs, by means of for instance, reducing turnover and absenteeism.

Such devices may also contribute to enhanced public health through health promotion and sensibilisation. Till (2018) relatedly argues that corporate wellness schemes and initiatives, that rely on employee data, are believed to have positive impact on productivity, and may have positive side effects on improving employee overall health. Critically, however, these opportunities may be presented as a means to support the employee experience or enhancing workplace wellness whilst in fact also providing 24/7 information about location, their activities, their mood, personal health and social life (Ajana, 2017). In a continued search for effectiveness and resilience through better use of good health data.

1.3 Community building and solidarity

In the third place, EW self-assessment tools may contribute to the creation of communities, or form feelings of solidarity (Ajana, 2017; Crawford *et al.*, 2015; Sharon, 2017; Wieczorek *et al.*, 2023). Engaging in self-tracking might additionally make it easier for users to become part of communities, both outside the workplace, but at the same time inside the workplace. The commonality of such a community, may be their shared orientation toward fitness or technological gadgets.

Gabriels and Coeckelbergh (2019) argue that analysing data about other users of self-tracking tech may create a feeling of proximity. However, community enacted through such means can be problematic and impinge on employees' privacy. However, it has been noted that a community centred around the sharing of data would be a narrow one (Ajana, 2017; Sharon, 2017), and one that is only based on particular parameters. For the WellFiciency-project, it should be questioned whether, how, to what extent and which parameters could be shared among colleagues. An enriched overview of colleagues' well-being data may enable a self-managing team to engage in data-informed discussions, potentially leading to (re)allocation of tasks and (re)scheduling of work.

In sum, the ethical affordances of employee well-being measurements - user empowerment, the promotion of health and well-being, and the strengthening of workplace solidarity - hold genuine potential for positive transformation. However, this potential is contingent upon meeting a range of ethical and privacy requirements. The remainder of this study is devoted to unpacking these requirements in detail, not to dismiss the concept of well-being measurement, but as a necessary step towards enabling it to function effectively, fairly, and in a way that truly benefits those it is designed to support.

2 ETHICAL CHALLENGES

Now that the advantages and the ethical affordances of EW self-assessment tools have been discussed, we continue with a list of notes on ethical challenges, including shortcomings and requirements, related to collection, storage, analysis and dissemination of employee well-being measurements. The list of ethical challenges consists of ten topics, being (1) social harm; (2) privacy and surveillance; (3) ownership, control and commodification of data; (4) autonomy; (5) data-facilitated harm; (6) datafication and interpretation of data; (7) negative impact on relation to oneself and to others; (8) possible shortcomings; (9) negative impact on health perception; and last but not least (10) unclarity regarding the legal framework, i.e. regulations and the enforcement of rules.

2.1 Enforced social harm

The first ethical challenge related to EW self-assessment tools is what Wieczorek *et al.* (2023) refer to as social harm. In the first place, social harm manifests in the context of norm-prescribing or norm-enforcing effects of tracking. Whereas tracking measurements may seem neutral, they are not. Their measurement present certain (ambiguous) thresholds and target scores that are predefined. These scores are typified as recommended, typical, optimal and may be seen as the green scores. Such desirable scores may seem standard, and thereby suggest that everything that falls outside of the range may be substandard, or abnormal. Management, or companies in general, may not disclose what these precise thresholds in their apps and devices are, however, these thresholds may set standards employees measure themselves with. One could question what and also who defines a threshold, and how it is defined. Moreover, whose data are seen as a standard measure? Authors in this area worry that the normative dimension of self-tracking devices can be internalised by workers, so that they would conform the threshold values endorsed by the applications and the devices (Ajana, 2017; Fotopoulou & O'Riordan, 2017) (Gertenbach & Monkelberg, 2016). This can be particularly harmful when employees - in the case of WellFiciency, industry operators - strive to meet standards or targets that do not align with their individual circumstances.

In the second place, employees accessing their EW self-assessment tools may continuously feel the urge to optimise their processes or their parameters. Deviating from the norm may be perceived harmful from an individual point of view, increasing anxiety or feelings of uncertainty.

Beyond that, EW self-assessment tools may be used to push through patterns of use, or patterns of behaviour that are deemed standard (Richardson & Mackinnon, 2018). This is, of course, influenced by those who are in power to control the information and data supply about the users' well-being parameters. Similarly, authors have voiced concern that the use of wearable tracking devices may shift the power relations in a way that is disadvantageous to the users, for instance, by giving employers access to the information about the employee – thereby empowerment would be concealed (Moore & Piwek, 2015; Moore, 2017).

2.2 Internalised responsibility

The second ethical challenge related to the internalisation of responsibility. The narrative of the literature is often that there is a sense of responsibility closely connected to EW self-assessment tools regularly and obligatorily: one is responsible to manage and check more and more personal parameters concerning one's own life. Those individuals that are not willing to self-track can be stigmatised as irresponsible (Lupton, 2016, 2018). Richardson and Mackinnon (2018) argue that the responsibility is steadily shifting from wider social, legal and institutional systems to individuals. One example is that operators who continuously feel exhausted because of regularly lifting heavy loads would feel their increased heart rates and physical demands are personal, and that they are personally responsible to lower these values (instead of questioning the organisation of work, or other systemic social causes as main predictors for these outcome values).

Furthermore, there is a risk that self-tracking tools place the burden of health solely on the individual. Staying healthy becomes primarily an individual responsibility, as the ability to self-monitor shifts the focus away from the surrounding healthcare system and onto the individual. Individualisation may posit a greater burden on individuals because self-tracking requires substantial effort (Morgan, 2016). Regarding the current WellFiciency-project, one could wonder how a recurring urge to looking at one's own well-being dashboard affects one's health. Can employees be held responsible to regularly check and not surpass certain values? And should we consider that such rates of responsibility affect operator well-being?

2.3 Constrained autonomy

The third challenge is the possibility of constrained autonomy. Authors note that the decision to adopt the EW self-assessment tools is not always entirely voluntarily, e.g. smartwatches or fitness wristbands may be given as part of workplace wellness, still, in that case workers could face direct and indirect pressure, e.g. shame and stigmatisation (Moore & Piwek, 2015; Moore, 2017; Oravec, 2020). Already in a private, non-working place context individuals may feel increasing pressure to engage in self-tracking and to share their data as these practices become more commonplace (Hull, 2017; Klugan, 2018).

Interestingly, this may also have repercussions for those willing to opt out of data sharing: these people may be stigmatised as selfish or as suspicious (Frank & Klinecewicz, 2018). Opting out of data sharing should be enabled in such a way that it won't raise suspicion, nor that the employee feels he or she needs to justify.

The line between what is voluntarily chosen and externally imposed is often blurred. Moreover, there may be loss of autonomy when users are forced or pressured to self-monitor their well-being. Importantly, the mere fact that these people, in the case of WellFiciency, industry operators, are wearing or using EW self-assessment tools may in itself affect operator well-being. Even though user autonomy, i.e. voluntary take up, may be high at the start, it can erode over time as for instance the data it collects influences users' decision making capabilities and behaviour (Danaher, 2018; Duus *et al.*, 2018). Another point is that when users' choices rely on their devices and the information these devices provide, they effectively delegate some of their agency to the technology. As a result, it can become difficult to assess the extent to which the devices influence users' decisions (Danaher, 2018; Klauser & Albrechtslund, 2014).

Users may feel their actions are not entirely their own, but shaped by the devices, especially when devices operate in an untransparent manner (Lanzing, 2016). Finally, authors observe that self-tracking wearables hollow out motivation, and that users engage in activities solely because of the high score that is attached to the activity within the application.

One more thing here is that data on individual employees' performance patterns, may be combined with other data obtained from emails and questionnaire response, etc. and eventually be used to feed algorithms that can send personalised messages to shape or nudge behaviour. Nudging messages may be prompt, demanding questions during one's shift, imposing to immediately respond (which may distract and affect task execution). On the other hand, nudging activities may encourage to stop conducting particular movements (which may not be possible during the execution of a particular task, and therefore send disparate signals to an employee, once again negatively affecting operator well-being). Lastly, one could question whether employees know they are being nudged, and whether they know which information is used, and how this affects their personal autonomy (or saves them from being manipulated) (Wakabayashi, 2018).

2.4 Data-facilitated harm

The fourth challenge is the risk for data facilitated harm. EW data can serve as a basis for both positively as well as discriminating against users, stigma within user groups. The possibility of discrimination based on EW data would then be a discussion that is based on individual health parameters, some of which may be affected by means of their task and job content, however, most of which may just be individual or personal traits or characteristics, personal resources and contextual characteristics.

Employers (or algorithms) may discriminate against employees whose data portrays them as less healthy or as less active than average, based on the data gathered (Challa *et al.*, 2017; Lanzing, 2016; Martin & Nissenbaum, 2016). Think for instance of employees with certain health risks (such as diabetes or such as suffering from insomnia). These employees may deviate in a significant way from threshold parameters. Their health risks may in the first place be revealed due to the dissemination of tracking data, and relatedly or unrelatedly affect organisational decisions in the second place. Interestingly, one could even discriminate against those individuals that opted out of sharing their own data. Ajana (2017) argued that aggregated data could foster discrimination against entire categories of people with comparable profiles. In that sense, one could discriminate against people that have not even shared their own data, and opted out of doing so. Although designed with good intentions, such as for instance, having impersonate and data-based HR decisions, rather than flawed, human based HR decisions. Still, machine learning systems trained to identify key patterns in company productivity based on ten years of data have been criticised for concluding that male candidates were overall superior (D'Astin *et al.*, 2018).

2.5 Datafied or reified employees

The fifth challenge is the risk for datafication or reification of individuals. The quantification of EW data and thereby the fundamental reduction of individuals or employees may be problematic in itself. The first argument is that the individual behind the data would be 'reified' or 'datafied', meaning that numerical data or numerical ways of expressing phenomena, in our case employee

well-being may be privileged to a proper understanding of employee concerns, employee well-being in itself. Often, the data that is generated is framed as objective and science driven, and therefore as authorised knowledge, while the embodied intuitive experiential ways of generating knowledge about the self would be neglected (Danaher, 2018; Hill *et al.*, 2019; Wieczorek *et al.*, 2023). Knowledge about oneself becomes numbers, thus the experience of the tracked task becomes the knowledge about how this task was experienced and may therefore become a skewed depiction of the actual phenomena (Moore, 2017).

This may lead to what Wieczorek *et al.* (2023) call a reduction of epistemic self-confidence, i.e. the idea that users would come to trust the data supplied by their devices over their own impressions and appreciation of the tracked activity, which may lead to users becoming alienated from their body and/or their senses (Danaher, 2018; Wieczorek *et al.*, 2023). Put simply, in the WellFiciency-project industry operators may over time start to rely more and yet more on their own well-being dashboards, and thereby alienate from their own well-being feelings.

Lastly, datafication, reification and even commodification takes place in case personal data is exploited by app developers. At the extreme, developers may want to generate profits based on user data, and capitalise on these data, via selling them to third parties, or by monetising it on their own through targeted advertising. Till (2014) argues self-tracking can be seen as an attempt to further deploy user data, and extract as much value as possible.

2.6 Data validity and reliability

The sixth challenge is that data from EW assessment tools sometimes proves to lack data validity and reliability. One could question to what extent employee data gathered fit the construct behind the data. This relates to data validity, or whether we measure what we want to measure. One could raise the question to what extent particular trends in the data truly cover trends in the experience of specific wearables users. Phenomena in reality are of course merely approximated by means of various data, and the question is whether and how fitting the transferability is, or to what extent the scale used or the physiological parameter measured covers a particular construct. Methodologically speaking, a particular method or measurement may not fully cover the construct that is to be measured. For instance, if we would systematically surpass one particular and significant dimension of operator well-being in the context of the WellFiciency-project, our measures will not be valid. This could cause serious harm to our findings and the implications we draw thereof.

Relatedly, employee well-being measurement data should provide solid, consistent and stable results. This relates to data reliability, or to how consistent and stable research results are if they were replicated. There is often little evidence supporting the claims of the device manufacturers regarding the accuracy of the devices, and this can be especially harmful in case of monitoring employee health and well-being (Gabriels & Moerenhout, 2018). As we are discussing employee health and well-being, both data validity and data reliability are concerns that should be further taken into account.

2.7 Flawed interpretability of well-being data

The seventh challenge is closely related to data validity and reliability, and purports to the proper interpretation of the collected EW data. In addition to questioning how well particular trends in the data truly cover trends in the experience of specific employees and how reliable these measurements are, one could also question the interpretability of well-being data. As we are discussing employee health and well-being data the quest to depict or represent employees' realities may be an ethical one.

One of the key promises of big data is the knowledge which may be gained from it. However, what if the knowledge gained from it is based on suboptimal, incomplete or poor quality data? In that case, we can expect problematic implications for the conclusions drawn (Jeske & Calvard, 2020). This challenge can be mitigated if a company carefully interprets the data.

Since the large volumes of data tend to be more unstructured than structured (Nunan and Di Domenico 2017), the effectiveness of analytics and algorithms depends on the quality of the data selected for analysis. Data will vary in how fully they capture the information necessary to answer all employer's questions.

Some problem solving may focus on aspects that are symptoms of, but not origins or root causes of this concern. Many workplace issues underlying employment relations are multidimensional, involving elements that are difficult to model - even with big data - because these dimensions are often intangible or not directly observable in the workplace.

Best case scenario is that best quality and high quantity of big data lead to cautious interpretation. Wieczorek *et al.* (2023) argue that analyses and results based on big data always need critical and well-informed revision, before concluding.

2.8 Reduced self-image

The eight challenge is that employees or individuals may experience negative effects on their relationship with themselves and with others. Self-quantification may spur them to become stressed or anxious about their results and their relation to what is considered standard or healthy (Baker 2020; Gabriels & Moerenhout 2018; Hopfgartner, Lomborg 2020). The measurements may fill employees with feelings of insufficiency and failure, and be harmful, especially in case users are already suffering from such feelings, like lower self-esteem.

Psychological states such as anxiety but also suspicion can arise when users of self-tracking devices feel their personal information might be disclosed to other people. This is especially the case if they are dispersed in great volume and in ways over which they have little or no control, such as in a workplace context. Some others argue that the increased use of self-tracking technologies promotes a radically individualistic stance (even narcistic stance) toward life, which can lead to a form of narcissism and egocentrism, focusing on the data limiting our view to approaching people as if they are nothing but an accumulation of data. As a result, users could be left with less influence over the image of themselves they project the world. The ways in which this affects employees' personal attitudes towards oneself and towards others should seriously be considered in the context of employee well-being measurements, as it may affect employees as well.

2.9 Lack of transparency

The ninth challenge is the lack of transparency in how the EW self-assessment tools have been designed and how they are being used. A shortcoming that pops up regularly, is that technology and system developers do not always disclose how their device algorithms operate (Crawford *et al.*, 2015). Conversely, they sometimes, whether intentionally or unintentionally, tend to withhold information that may be valuable or relevant from the user's perspective.

Even despite consent forms, it remains sometimes impossible for users to know how and why their data is used, as well as to give meaningful consent to the practices or to the flow of their data. Consent may be a desirable and valuable component to any data collection effort. The value of consent is undeniable, even in case it may not explicitly be required or expected, still, employees should be aware of how their data is being tracked, to what extent. They should be able to easily understand exactly which data they have given their consent to being collected, and in cases of opting out, denial, or withdrawal of consent, employees should obtain verification about this. In case of changes in the patterns of data collection, transparency should be guaranteed by means of renewed consent forms (Jeske & Calvard, 2020).

Lacking transparency may be perceived by employees as unfair and thus encounter resistance to participation or acceptance whichever wearable tracking device. Manyika (2019) argues at the same time there is also a lack of clarity in how to define measures of fairness (Manyika, 2019). Transparency should be taken seriously, since employees still have a lack of trust in people analytics' outcomes. A study concluded that 63% of the companies' employees believe their employer is collecting too sensitive data, and about 72% believe their companies are not telling them what data they are collecting (Pease 2018). The use of wearable technology to monitor and track workers may also have a negative effect on safety management and safety culture. Hovden *et al.* (2010) provide an example of using cameras to monitor work for decision support in three Norwegian offshore oil and gas concerns. Acknowledged monitoring in these cases lead to workers feeling uncomfortable at being evaluated all the time and even result in a sense of mistrusting their employment relationship.

2.10 Regulative framework

The tenth challenge relates to regulations and the enforcement of rules. The ethical challenge here is that all articles we consulted argue there is a relative lack of regulation on these tracking technologies (Kleinpeter, 2017; Lanzing, 2016; Martin & Nissenbaum, 2016; Moore & Piwek, 2015; Oravec, 2020). Since technologies are evolving so rapidly in ways that are difficult to anticipate, this raises pressing questions for HR practitioners: What to do in new situations that are not covered adequately by legislation? Plus, what may be legal is not autonomically ethical. This is particularly problematic when it comes to health and well-being monitoring devices.

In many countries, such devices face additional regulatory scrutiny; however, a clear and robust overall framework is still lacking. Even if there are laws in place that could protect users from potential negative impact of EW measurement technologies, government institutions may not always be prepared to enforce them or even willing to do so. Different data regulatory regimes across countries make it particularly relevant as data is often transferred from users in EU to corporations in US where not much of regulations are at stake, and where there is far less data

protection legislation (DPL). Few organisational and professional codes of conduct deal with best practices for using self-tracking data in a workplace environment and those that exist might not be sufficiently established. As a result, the kinds of decisions motivated by self-tracking data and their impact on employees may be varying greatly depending on the employer and his or her ethical standards.

In the EU, the General Data Protection Regulation (GDPR) has started to guide vendors and users of various data tracking innovations in addressing their vulnerabilities; however, it leaves gaps that require the development of ethical guidelines. (Hamilton & Sodeman, 2020). Moreover, while GDPR represents a significant advancement of employee rights in the digital era, its primary focus on protecting personally identifiable data leaves open questions around the uses of anonymised or non-identifiable data, for which breaching GPDPR may impose severe penalties, failing to safeguard or misuse personal information (Mann & Matzner, 2019; Tursunbayeva *et al.*, 2018).

Outsourcing data services to third party vendors will change the dynamics of how employers share legal responsibilities with these vendors for data analytics storage and ownership as well as the sharing of data integration and conversion costs. External data analytics providers cannot entirely reduce employers' legal responsibilities towards safeguarding employee data. There will be always a risk of ambiguity or lack of shared responsibility for addressing the threats and fallout related to big data and data accidents (Nunan & Di Domenico 2017). Many stakeholders do not feel responsible for managing risks unless they have a personal connection to the data or have been directly impacted by privacy regulations.

In line with legal requirements organisations should always inform their employees of their right to opt out of relevant data collection processes and give them the opportunity to do so. For instance, the right to informed consent is part of the privacy guidelines from OECD. Additionally, organisations need to consider whether employees are making choice to participate freely (Mann *et al.*, 2018).

2.11 Ownership, control and commodification of data

The question of who owns the data remains to some extent unresolved and controversial. Users might not have insight into what is and is not collected (Lupton, 2018; Piwek *et al.*, 2016). As well as what are their legal rights related to self-tracking data, especially as companies have commercial motivations to bind the generated data to their products (Till, 2019), and prepare legal documents regulating the ownership and use of data in ways that give them the most power over it (Kreitmar & Cho, 2017). The data should be considered as 'child' of the user and the company supplying the device (Wieczorek *et al.*, 2023).

Unclear structure of data ownership is seen as giving companies near full discretion over how and with whom data is shared. Access to data is often granted to third parties which in their view could be problematic as users may be unaware and unable to control who uses or exploits their data and for what purposes. If users were granted more control over or insight into how data is shared it could increase disclosure of sensitive information as users could be manipulated into consenting to share data or they might not realise the consequences of their consent. Nevertheless, users cannot take it for granted that third parties that gain access to personal data will manage it in ethical and responsible ways.

In workplace contexts in particular, employees should be able to exert control over their personal data and about the extent of the potentially excessive knowledge they provide about their lives (Moore & Piwek, 2015). Klugman (2018) notes the issue of access to personal self-tracking data could be contentious, as exemplified in the healthcare context as well, since patients are sharing their data often voluntarily, with third parties that include healthcare providers, device manufacturers and friends and family, think for instance of electronics health records (EHRs).

2.12 Privacy

Anonymising user data in aggregated datasets is widely regarded as common practice. However, this is often seen as insufficient for protecting users' privacy, as the data can be easily re-identified (Ajana, 2017). In the case of the WellFiciency-project, the connection between the collected employee data and the individual employee remains effectively inescapable. Can we encrypt the data in such a way that one can no longer deanonymise it? Or should we grant access to a single actor in the organisation who can make use of the non-anonymised data?

However, it should thus be questioned at what point privacy is breached. Individuals may for instance be contributing to larger data sets and thereby to colleagues' personal information. Based on anonymised inference conclusions about colleagues may unwillingly be drawn. Even if privacy breaches do not lead to direct user harm they can still violate users' contextual expectations relating to personal information. Even though the employee agrees with the anonymised data collection he or she may feel uneasy or insecure in case certain relationships and connections between his or her personal data are personally being exposed. Additionally, it has been observed that privacy violation can be particularly problematic in case wearable tracking technologies collect highly sensitive information such as mental and physical health and well-being data.

Moreover, the increased adoption of self-tracking technologies can change the general attitude in the organisation of deployment, and more particularly, the attitude about the privacy. Privacy is often framed by developers as a concept that privileges the individual values over public goods. As such, Morozov (2013) points at the increasing popularity of self-tracking and that it may result in a situation where collection and sharing of data will become the norm at the expense of those who actually want to preserve their privacy.

Particularly in the workplace, privacy raises pivotal concerns for employees and employers. Employees expect to be in control of the personal information and access they provide to the organisation. Employers, however, expect extensive information regarding their employees as well as extensive access to employees' presence (Bhave *et al.*, 2020). To a certain extent, organisations evidently have the right to collect information about their workforce. Through the course of the employment relationship, organisations do, sometimes incontrovertibly, need information regarding the ability, the motivation and the performance of their employees (Culnan, Smith & Bies, 1994). So, the intuitive thought that all data needs to be anonymised in organisations is false as well.

Privacy has been a much disputed concept in organisation studies, now with the emergence of tracking tools, gaining more and more attention, since technological advances are outpacing our understanding of the privacy implications. Interconnectedness of employee data will generate tremendous amounts of data that can provide information on employees' health, time use and

productivity across the work and home domains (Bhave *et al.*, 2020; Stone & Stone-Romero, 1998).

2.13 Surveillance

A final ethical challenge, related to privacy, widely discussed by authors is the issue of workplace surveillance through employment of workplace schemes and wearable devices that are mostly designed to monitor the activity and productivity of employees (Moore & Robinson, 2016; Zuboff, 2019). Sometimes, such wearable devices go as far that they are monitoring employees wearing the technologies outside the workplace, to even monitor leisure time (Moore & Robinson, 2016; Wieczorek *et al.*, 2023). This reminds of Michel Foucault's concept of biopower and sousveillance, or the idea of bottom up monitoring done by the citizen, and the monitoring of other people by their peers, respectively. Translated to the workplace, even though the employer may not be given access to the employee health and well-being data, their colleagues and their team manager may be given access to it. This idea of sousveillance may be less constricting compared to surveillance.

In a workplace context, surveillance technology refers to the use of various tools and systems to monitor employee activities, behaviours, and interactions within the workplace environment. Motives lie in a power base of control and manipulation of a submissive workforce, rather than supporting and listening to a workforce that is trying to meet organisational goals without compromising their own safety, health and well-being. According to Foucault, surveillance is what the technology becomes, it is a function of power that continually polarises between power enhancement and powerlessness (Foucault as cited by Paramore 2015). Technologies that allow to be logged in at and sometimes even outside work enable employees to be viewed by supervisors and also create a panopticon effect, reducing workers' experienced privacy and autonomy, potentially negatively affecting job satisfaction and employees' mental health (Booth, 2019). One academic experiment revealed that the prospect of active monitoring reduced potential employees' impressions about the organisation's ethics as well as the likelihood of job acceptance and job satisfaction (Holt *et al.*, 2017)

Interestingly, narratives in the grey literature, most often industry sources suggest that most employees are accepting of digital monitoring. For instance, in a blog for the academy to innovate HR, it has been argued that this acceptance is a result of organisations' success in persuading employees that sharing personal information is in their interest, thereby reframing workplace monitoring from an authoritarian practice to one with an ostensibly participatory character (Wartzman, 2019) or to participatory surveillance (Marchant, 2019).

The extent of surveillance and its relatives sometimes have a far-reaching stretch. Employee wellness programs for instance represent a particular class of workplace monitoring which may require staff in some cases to share their medical data, wear a biometric monitoring device or even to be microchipped (Jacobs, 2017).

Even strong opponents of monitoring such as the American civil liberties union acknowledge that employers have a right to undertake some monitoring (Kim, 2017), however, it always calls for ethical standards. Guidelines then always are that employees are informed about the monitoring system, and that performance benchmarks are set, using documentation or records for benign purposes rather than for sanctions.

3 CONCLUSION

Based on a review of both academic and grey literature on EW assessment tools, we conclude that ethical opportunities are likely to flourish only if the majority of ethical challenges and drawbacks are effectively addressed. This overview identifies and elaborates on three key ethical opportunities: user empowerment, promotion of health and well-being, and community building and solidarity. At the same time, we highlight a range of potential ethical risks and negative outcomes, including social harm; privacy violations; issues of control and commodification of data; constrained autonomy; data-facilitated harm; excessive datafication and automated interpretation; adverse effects on self-perception and interpersonal relationships; misrepresentations of health; and, importantly, a lack of clarity regarding the legal framework, including regulations and their enforcement.

References

Ajana, B. (2017). *Digital health and the biopolitics of the Quantified Self. Digital Health*, 3, 2055207616689509.

Bal, M., Vermeerbergen, L., & Benders, J. (2023). Putting head-worn displays to use for order picking: a most-similar comparative case study. *The International Journal of Logistics Management, 34*(5), 1475–1499.

Bhave, D. P., Teo, L. H., & Dalal, R. S. (2020). Privacy at work: A review and a research agenda for a contested terrain. *Journal of Management, 46*(1), 127–164.

Challa, N., Yu, S., & Kunchakarra, S. (2017). Wary about wearables: potential for the exploitation of wearable health technology through employee discrimination and sales to third parties. Intersect: *The Stanford Journal of Science, Technology, and Society, 10*(3).

Crawford, F., Cezard, G., Chappell, F. M., Murray, G. D., Price, J. F., Sheikh, A., Simpson, C. R., Stansby, G. P., & Young, M. J. (2015). A systematic review and individual patient data meta-analysis of prognostic factors for foot ulceration in people with diabetes: the international research collaboration for the prediction of diabetic foot ulcerations (PODUS). *Health Technology Assessment (Winchester, England), 19*(57), 1–210.

Danaher, J. (2018). Toward an ethics of AI assistants: An initial framework. *Philosophy & Technology, 31*(4), 629–653.

Duus, R., Cooray, M., & Page, N. C. (2018). Exploring human-tech hybridity at the intersection of extended cognition and distributed agency: A focus on self-tracking devices. *Frontiers in Psychology, 9*, 351016.

Elms, H., Johnson-Cramer, M. E., Berman, S. L., & Phillips, R. (2011). Bounding the world's miseries: Corporate responsibility and Freeman's stakeholder theory. *Stakeholder Theory: Impact and Prospects*, 1–53.

Fotopoulou, A., & O'Riordan, K. (2017). Training to self-care: Fitness tracking, biopedagogy and the healthy consumer. In: *Self-Tracking, Health and Medicine* (pp. 54–68). Routledge.

Gabriels, K., & Coeckelbergh, M. (2019). 'Technologies of the self and other': how self-tracking technologies also shape the other. *Journal of Information, Communication and Ethics in Society, 17*(2), 119–127.

Gabriels, K., & Moerenhout, T. (2018). Exploring entertainment medicine and professionalization of self-care: interview study among doctors on the potential effects of digital self-tracking. *Journal of Medical Internet Research, 20*(1), e10.

Hamilton, R. H., & Sodeman, W. A. (2020). The questions we ask: Opportunities and challenges for using big data analytics to strategically manage human capital resources. *Business Horizons, 63*(1), 85–95.

Hill, P. L., Edmonds, G. W., & Hampson, S. E. (2019). A purposeful lifestyle is a healthful lifestyle: Linking sense of purpose to self-rated health through multiple health behaviours. *Journal of Health Psychology, 24*(10), 1392–1400.

Hovden, J., Albrechtsen, E., & Herrera, I. A. (2010). Is there a need for new theories, models and approaches to occupational accident prevention? *Safety Science, 48*(8), 950–956.

Jeske, D., & Calvard, T. (2020). Big data: lessons for employers and employees. Employee Relations: *The International Journal, 42*(1), 248–261.

Klauser, F. R., & Albrechtslund, A. (2014). From self-tracking to smart urban infrastructures: Towards an interdisciplinary research agenda on Big Data. S*urveillance & Society, 12*(2), 273-286.

Kleinpeter, E. (2017). Four ethical issues of 'E-Health'. *IRBM, 38*(5), 245–249.

Lanzing, M. (2016). The transparent self. *Ethics and Information Technology, 18*, 9–16.

Lupton, D. (2016). *The quantified self*. John Wiley & Sons.

Lupton, D. (2018). How do data come to matter? Living and becoming with personal data. *Big Data & Society, 5*(2), 2053951718786314.

Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society, 6*(2), 2053951719895805.

Marchant, G. E. (2019). What are best practices for ethical use of nanosensors for worker surveillance? *AMA Journal of Ethics, 21*(4), 356–362.

Marler, J. H., & Boudreau, J. W. (2017). An evidence-based review of HR Analytics. *The International Journal of Human Resource Management, 28*(1), 3–26.

Martin, K., & Nissenbaum, H. (2016). Measuring privacy: An empirical test using context to expose confounding variables. Colum. *Sci. & Tech. L. Rev., 18*, 176.

McAleenan, P., McAleenan, C., Ayers, G., Behm, M., & Beachem, Z. (2018). The ethics deficit in occupational safety and health monitoring technologies. *Proceedings of the Institution of Civil Engineers-Management, Procurement and Law, 172*(3), 93–100.

Moore, P., & Piwek, L. (2015). *Unintended consequences and the dark side of the quantified self.* Sustainable Societies Network Commissioned Paper.

Moore, P., & Robinson, A. (2016). The quantified self: What counts in the neoliberal workplace. *New Media & Society, 18*(11), 2774–2792.

Moore, P. V. (2017). *The quantified self in precarity: Work, technology and what counts.* Routledge.

Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism.* PublicAffairs.

Oravec, J. A. (2020). Digital iatrogenesis and workplace marginalization: some ethical issues involving self-tracking medical technologies. *Information, Communication & Society, 23*(14), 2030–2046.

Piwek, L., Ellis, D. A., Andrews, S., & Joinson, A. (2016). The rise of consumer health wearables: promises and barriers. *PLoS Medicine, 13*(2), e1001953.

Richardson, S., & Mackinnon, D. (2018). Becoming Your Own Device: Self-Tracking Challenges In The Workplace. *Canadian Journal of Sociology/Cahiers Canadiens de Sociologie, 43*(3), 265-289.

Sharon, T. (2017). Self-tracking for health and the quantified self: Re-articulating autonomy, solidarity, and authenticity in an age of personalized healthcare. *Philosophy & Technology, 30*(1), 93–121.

Sharon, T., & Zandbergen, D. (2017). From data fetishism to quantifying selves: Self-tracking practices and the other values of data. *New Media & Society, 19*(11), 1695–1709.

Stone, D. L., & Stone-Romero, E. F. (1998). A multiple stakeholder model of privacy in organizations. In: *Managerial ethics* (pp. 45–70). Psychology Press.

Till, C. (2019). Creating 'automatic subjects'*: Corporate wellness and self-tracking. Health, 23(*4), 418–435.

Tursunbayeva, A., Di Lauro, S., & Pagliari, C. (2018). People analytics—A scoping review of conceptual boundaries and value propositions. International *Journal of Information Management, 43*, 224–247.

Tursunbayeva, A., Pagliari, C., Di Lauro, S., & Antonelli, G. (2021). The ethics of people analytics: risks, opportunities and recommendations. *Personnel Review, 51*(3), 900–921.

Wakabayashi, D. (2018). *Uber's Self-Driving Cars Were Struggling Before Arizona Crash.* International New York Times, NA-NA.

Wartzman, R. (2019). Workplace tracking is growing fast. Most workers don't seem very concerned. *Fast Company*, 20.

Wieczorek, M., O'Brolchain, F., Saghai, Y., & Gordijn, B. (2023). The ethics of self-tracking. A comprehensive review of the literature. *Ethics & Behaviour, 33*(4), 239–271.

Zuboff, S. (2019). Surveillance capitalism and the challenge of collective action. *New Labor Forum, 28*(1), 10–29.

PART 2
INTERVIEWS

Introduction

The aim of this second part is continue researching the ethical and privacy related considerations, deepening and applying the results we brought about in the literature review. The focus of this second part is just as the first one on the applying these considerations to the WellFiciency-project.

The third part of the report both deepened and applied the results from literature review by interviewing 23 experts and stakeholders with varying backgrounds (Table 2.1). In addition to the dimensions that were referred to in the first part of this report, expert and stakeholder interviews allowed us to surface new ethical and privacy related aspects, and at the same time enabled us to nuance the ones that were already present. A first conclusion is that the topics of worker participation and involvement should be treated as *transversal* initiatives throughout the entire technology timeline. These initiatives are to be taken into account as from the developmental phase of the assessment tool. A second conclusion is that the existing workplace context (e.g. the employment relations and the existing collaboration between employer and trade unions) will play a quintessential role in the development, implementation and adoption of such initiatives. A third conclusion is that the existing legislation on employee well-being, data protection legislation and new technologies at work should be taken into account. The difficulty here is that this legislation is present at different levels (EU, national, sectoral, and workplace level). A fourth conclusion is that the methodological challenges may go beyond what the literature anticipated. Lastly, we distinguish different parties that are to be taken into account and consulted when deploying such a EW assessment tool.

1 METHOD

The research outlined in this part adopts a qualitative approach, using 23 semi-structured interviews to explore the ethical, privacy related and also legal considerations involved in the collection, storage, analysis and dissemination of employee data within organisational contexts. The goal is to identify and analyse the potential barriers and challenges organisations face when managing employee data, particularly regarding privacy, legal compliance, and ethical concerns.

The data collection method consists of a series of 23 in-depth interviews with key stakeholders from diverse backgrounds (Table 2.1). These interviews were conducted with representatives from various sectors, including third-party service providers, regulatory bodies, health and safety stakeholders, technological and data tools specialists, external experts, legal experts, as well as international stakeholders. The idea was that each of these participant brought a unique perspective on the ethical, privacy and legal, but also practical considerations of handling employee data within organisations.

The interview followed a three-step structure: at the start, the questions were predominantly open-ended and loosely structured; subsequently, research findings from the literature (as outlined in Part 2) and the WellFiciency project context were presented; finally, this formed the basis for a more in-depth exploration of the topic in relation to defining project and use case requirements for WellFiciency. The interview guide was informed by the results of an extensive literature review that examined both generic ethical requirements for data handling and specific legal concerns related to privacy in the workplace. The methodology aimed to capture not only the regulatory and legal aspects but also the broader ethical and practical considerations that may impact the implementation of well-being data collection and processing systems in organisations. The semi-structured nature of the interviews allowed for flexibility in responses, enabling the exploration of unforeseen topics and nuances that emerged during the conversations.

The data from these interviews were analysed thematically to identify common barriers, ethical concerns, and practical challenges across the different sectors and stakeholders involved. By comparing insights from various experts and sectors, the research highlights the intersection of ethical considerations, legal compliance, and practical challenges organisations face when managing employee data. The results of this research aim to contribute to the development of best practices for ethical data management in organisational contexts, with a focus on ensuring compliance with privacy laws while addressing the concerns of various stakeholders.

Our findings throughout all what follows are supported by interview quotes, as is often the case in qualitative studies to support our statements and to be in accordance with a narrative approach. These illustrative quotes were all translated to English, and are supported with the initials and organisation

TABLE 1.1 Table of Interviewees

N	Name	Expertise	Organisation	Interview date
1	AP	Legal (EU)	ETUI	27/05/2024
2	OS	Legal (BE)	ALAW	31/05/2024
3	AS	Ethical (EU)	EU OSHA	12/06/2024
4	MC	Ethical (EU)	EU OSHA	12/06/2024
5	DDB	Ethical (BE)	FOD WERKGELEGENHEID	21/08/2024
6	JV	Union (BE)	ACV METEA	20/06/2024
7	KR	Union (BE)	ACV	27/09/2024
8	PVDB	Legal + Union (BE)	ACV	01/10/2024
9	LT	Union (BE)	ABVV	01/10/2024
10	P	Union (BE)	ABVV	10/10/2024
11	DVC	Union (BE)	ABVV	11/02/2025
12	LT	Practitioner	XSENS	13/02/2025
13	KDM	Union (BE)	VBO	13/02/2025
14	RH	Ethical (BE)	VUB	25/10/2024
15	DG	Legal + Ethical (EU)	UGENT HIVA	17/10/2024
16	ST	Legal + Ethical (BE)	KU LEUVEN	17/10/2024
17	KD	Practitioner	VBO	22/04/2024
18	MM	Legal (EU)	KU LEUVEN	29/03/2025
19	AL	Research (BE)	KU LEUVEN	23/4/2025
20	KD	Practitioner	YSENS	21/4/2025
21	JM	Practitioner	ZSENS	28/4/2025
22	GM	Research	KU LEUVEN	29/4/2025
23	MV	Research	UGENT	06/5/2025

Note: The names of all interviewees have been pseudonymised and are represented using their initials.
ALAW is a fictitious name of a lawyer company
XSENS, YSENS and ZSENS are fictitious names of practitioners' organisations.

2 RESULTS

The findings of the series of interviews are structured as follows. First, all ethics regarding the process *towards* the implementation of a technological methodology are introduced. Second, the ethics related to the outcomes of our measurements are mentioned. Third, we tap into the work-place ethics by looking at the adversary or complementary interest of operators and their managers. Fourth, the legal aspects follow. Fifth, methodological challenges follow. Sixth, we bring about contextual aspects that influence the privacy and ethics of data collection in the context of well-being at work (e.g. sectoral, national, cultural differences). Lastly, we list all relevant parties that were named during the interview and bring about quotes to illustrate the attitudes of the interviewees about the roles these parties should take.

2.1 Ethical considerations in the process of developing and implementing the assessment

2.1.1 Ethics on the technology timeline and the *stakeholder journey*

According to four respondents the successful implementation of the WellFiciency methodology will, just like with all new technologies, largely depend on the **early involvement of end users and stakeholders**, in this case operators and also their representatives. In case the project provides early and transparent communication and in case operators are (widely) informed from the start, this may reduce suspicion and resistance and increase their motivation to be involved, and eventually their rates of acceptance. If, in contrast, communication and involvement happens too late (or not satisfactorily), employees may push back against changes they feel were imposed without their input.

If I only find out afterwards […], resistance will arise […]. So actually, how the report from the prevention service should be communicated to inform you in advance. – AP (ETUI)

To improve adoption, researchers, practitioners as well as unions stressed to as early as possibly **involve all stakeholders proactively**, by means of both direct and indirect participatory approaches, and ensure that not only the final technological methodology, but also the process towards the technological methodology aligns with employees' actual needs and concerns. The latter point is often seemingly self-evident, however, the needs of operators, their wishes and their expectations should be nicely taken along.

A common issue is that decisions are sometimes made, that the experimentation has already been done, and that funds spent before identifying the real problems in practice, which in turn is often leading to challenges during the design and implementation of new technologies.

Often, the opposite happens—nothing is done initially. And only during implementation problems arise. But by then, the money has already been spent. The consultants have already left. – KR (ACV)

More so, although researchers and employee representatives clearly stressed the benefits of an **open ended approach** (both for the eventual users, as for the other stakeholders, but also for the final outcomes of their imagined product), the open ended approach is often not done satisfactorily. Instead, the open ended approach is often surpassed by the rapid and result-driven intentions of management. Research, however, has shown that open-ended processes of new technologies result in better use outcomes. This is beautifully exemplified by the following quote:

On the one hand, you have got pressing managers who think they must achieve a certain result by a certain date for a certain amount of money. On the other hand, you have got managers that are anything but result-oriented. For the latter it is much more about identifying the problem than it is about solving the problem. – RH (VUB)

Interestingly, when it comes to digitisation at work, one of the interviewees mentioned to having been involved in the *European Social Partners Framework Agreement on Digitalisation* that precisely stresses this **process-oriented approach** which surpasses the rigid employer-employee rules and regulations. Throughout the entire process, starting with privacy by design all agreements highlight principles like privacy, human control, adapting to the needs of different industries and company sizes.

Four transversal attention points in this framework agreement are: human in control principle, privacy, right to connect and disconnect. They are transversal since they are included in every step of the process of design and implementation. But it's not that the framework agreement is really a written step-by-step plan: it depends on the nature of the company, the size of the company. That all plays a role. But it is an agreement that actually, at the national level, and at the level of countries and sectors, should encourage action. – KDM (VBO)

The goal is to encourage sectors to actively engage with these frameworks and enable companies and operators to jointly identify needs, particularly regarding well-being issues. This collaborative approach aims to optimise the design of the technological methodology, support smoother implementation and acceptance, and ultimately improve operators' well-being outcomes. It takes in other words a temporal strategy, and one that flexibly adapts to the needs of evolving technological methodology, and its users (and other stakeholders).

In the interviews conducted, **several key concerns** are raised regarding the involvement of workers in the design and implementation of tools and technologies. For instance, a research expert from ETUI emphasised many tools are designed primarily with the employer's perspective in mind, and not for worker protection. More so, this person argued that **without workers' input** in the design process, these tools cannot serve as effective means of protection. This person therefore highlighted the importance of incorporating worker input and validated parameters into

these tools for them to be truly beneficial. An interviewed EU OSHA expert mentioned and stressed the concept of 'privacy by design,' which considers privacy as an integral part of the development process.

The software development requires knowledge of what happens at computational level. We should questions whether workers will be able to participate meaningfully here – AS (EU OSHA)

The research expert from ETUI stressed it is a challenge in determining whether workers have the necessary skills and knowledge to influence the design of products. This person acknowledged that some workers may have the expertise to do so, but others may not, raising questions about the extent to which worker input can be integrated **meaningfully into the development process**. A last complaint on the lack of involving operators meaningfully, relates to the role and power industry players have in these matters.

2.1.2 Ethics on worker *participation*

The section focuses on the challenges and considerations surrounding worker participation in decision making processes related to technology design, technology adoption and technology use in the workplace.

When it comes to **meaningful participation**, it goes beyond designing with the worker in mind, but instead, it is about guaranteeing that workers are around the drawing table. Workers often do not have the power to negotiate the parameters or decide on the data embedded in workplace tools, especially when these tools are developed by third parties for employers to boost productivity. This **lack of control** makes it difficult for such tools to truly serve worker protection unless they are designed with direct worker input and validated parameters. In some cases, employers may **underestimate workers' knowledge and ability** to contribute meaningfully to discussions about technology implementation, especially in industrial settings. While some companies are **open to worker feedback**, others view it as **unnecessary or burdensome**. There is a need to strike a balance between efficiency and worker engagement to ensure that workers are not just consulted but truly involved in shaping workplace technology.

This is why they cannot really be used for worker protection, unless, as I said before, they are designed for workers with workers inputs and with parameters that are validated by workers, metrics and parameters. – AP (ETUI)

While workers may be invited to provide input, their participation often isn't **meaningful.** In many cases, workers are only consulted during one phase of a process, and their suggestions may not be integrated into the final design. This limited involvement can lead to ineffective or harmful outcomes, with companies potentially shifting blame onto workers for not participating fully. To be more specific, the difference between **consultation and true involvement** is critical. Even if workers are consulted or invited to participate, their input may not influence the final product. Workers' concerns may be disregarded, leading to frustration and lack of ownership over the tech-

nology. This also raises questions about how to measure the effectiveness of worker participation and ensure it has a tangible impact on the final outcome.

You can bring all the workers that you want, right? But their involvement is it going to be meaningful? Are their suggestions going to be taking all along the development of the product or only just one phase? […] Companies will have a lot of arguments to say you were involved. You had the chance to speak. You were consulted. You didn't do it. That's not my fault. This is what happens. – RH (VUB)

Some people are sensitive to it and would rather not cooperate, while others are open to it and will probably be cooperative. So in that sense, yes, thank you, it is easiest to be direct and open about everything, and when people receive information, they are much more likely to be open to certain things if it is clear. So I would definitely focus on having something in writing for them to sign when consent is requested, along with a privacy policy, where they either accept it or simply indicate that they have read or been informed about it. They don't have to accept it, but they must acknowledge it. – LT (XSENS)

Workers are more likely to engage if they understand why data is being collected and how it will be used. Transparency about data collection is crucial to building trust and ensuring that workers feel informed and involved. Without this, participation may be hindered, as workers may be sceptical or unwilling to engage in processes they don't fully understand. Transparency is one thing but data literacy, and data awareness are fundamental issues to have proficiency in. While there are efforts to involve workers in the development and implementation of technology, meaningful participation remains a challenge. Employers must ensure that workers' input is **not only sought but also acted upon** to create tools that genuinely benefit both workers and employers. Without this, the risk of ineffective tools and low rates of acceptance increases.

In the interviews the question was raised to what extent workers are ideally involved in this trajectory, whether there are general rules of thumb that we as a research team have to take into account. The quote by the researcher below nicely illustrates that this is a difficult point, that has been discussed multiple times.

The problem with those operators is that they have to work, right? It also works or turns when you ask them those questions for a study, it's a moment when they are working in the factory or workshop where they are. It doesn't matter much if they can be consulted here, but ideally, you would have in an SBO some kind of sounding board or advisory council. And ideally, there would be someone from those operators who can actually see on that level if this is going in the right direction or not. Or I see it this way: we talk a lot about the category of operators with all kinds of experts, while they themselves are not really given the space to explain their own opinions in their own words. So, that will be the difficult part, I think. – RH (VUB)

Interestingly, one of the researchers argued that **worker participation in itself** may be related to mental health and well-being. From the literature on organisational change management, we know that change often causes workers to resist, and that change may have severely bad impact on

workers well-being. The same goes for this trajectory of technological change, or of initiating a technological tool. The practitioner interviewed, below, discusses that worker participation in itself has the potential to affect the well-being of operators.

Well-being is actually the basis for going into dialogue. This also has to do with mental health for me. And that you really need to involve them completely, and I think that if you don't involve an operator, then maybe you've solved the problem of the defect on the line, so to speak, but now you've solved the problem of involvement of the employee with the company. There is a sense of ownership and the employee stays here working for years with a lot of pleasure and with a certain sense of bliss. So, and ultimately, what is the goal? Preventing turnover at the end of the day, right? – MC (EU OSHA)

Lastly, the person from the social partners argued boldly that participatory approaches aren't the holy grail either.

It's also a cliché to say, 'Yes, but the employee themselves knows best their risks and challenges at their workstation.' That's also a cliché that is often not true. The driver, for example, doesn't necessarily know everything about the mechanics of the vehicle where the issue lies. And there are a thousand examples like that. So for me, participatory means simply involving everyone at their level and with the knowledge and capabilities they have, but don't assume ... – social partner KDM

While it would indeed be unreasonable to expect every worker to fully grasp the technological details of the tools they use, the participatory approach could still focus on discussing key design options and their implications for control, task content, and job quality.

2.1.3 Ethics on stakeholder-based *communication*

A practitioner and researchers highlights the importance of adapting communication to different audiences within an organisation. Operators, for example, require direct feedback and simple explanations, without too much technical detail. Preventive advisors can only focus on a few key topics before losing interest, particularly in areas like digital ergonomic risk analyses or structured checklists. higher-level executives, such as operational directors or CEOs, respond well to discussions about ROI and decision making insights.

We need to tell a different story depending on who we have in front of us, because otherwise, we actually make some people too uncomfortable. That is really quite a thing. Yes, unfortunately. – Practitioner LT

A major challenge in communication is that improving processes is often not considered part of the job for many employees - they focus on identifying problems rather than solving them. This lack of structured follow-up makes change difficult. The key takeaway is that messaging must be **tailored to different stakeholders** to ensure engagement. A one-size-fits-all approach can make some

people uncomfortable, so speaking the 'language' of each audience helps bridge gaps within an organisation. It is both identifying the languages in the organisation, on the one hand, but more importantly even is it to bring together the different interests. This practitioner as an outsider to the organisation argued that …

As an outsider who maybe only comes in temporarily, you actually ensure that different parties and organisations at different levels somehow come together by speaking those different languages yourself. That is really very fascinating. – LT (ACV)

One employee representative (ACV – EP) argued that the main communication is not so much about operator or employee well-being (not so much about the soft topics), but instead about wages and other working conditions (thus, generally about the harder topics). Here, I add that a representative (ABVV) argued that there is, however, growing interest in improving workplace well-being, but that mainly communicating and motivating all stakeholders remains a challenge.

2.1.4 Ethics on budget allocation

In four interviews, operator well-being was closely related to **budgetary initiatives**. Interestingly here is that some sectors have pre-allocated budgets (a percentage of previous year's payroll) to improve working conditions. This freed up budget makes discussion on potential solutions easier. Still though, for many initiatives companies must personally invest in preventive measures, which is when financial concerns become a barrier. Many initiatives remain largely unimplemented due to a reluctance to allocate additional funds.

So we organised an initiative, one that was fairly completely free for the companies, and you will surely know that if you have to pay for it yourself, it does cost quite a bit of money, right? We have, with great regret, had to conclude that there was actually too little interest from companies to participate in large numbers, so yeah. – DVC (ABVV)

More so, much of the allocation of budgets goes out to social partners *diagnosing* well-being issues, and to consultants and developers *implementing* new technologies. However, having contributed significantly to these parties on either new technologies, or new initiatives, they receive little in return, often leading to cynicism and low engagement. The following quote nicely exemplifies that the project may already have run out of costs

Having run out of cost early in the process, innovative solutions are proposed, companies immediately seek funding through social partners, but rigid financial structures and a lack of collaboration limit access to these funds. More so, there are **small budgets** available for topics like ergonomics make it difficult to integrate external solutions into existing frameworks.

Improving health and well-being has a cost. […] This protective equipments are expensive, I mean health, it takes a cost. Uh, maybe we need to have two checkups by private institutions per year. The company has to pay the private checkups of all the staff. It's a lot of money. Many companies do not have this private medical checkups for their staff. – MM (ETUI)

2.2 Ethical considerations on the outcomes resulting from measurement

2.2.1 Ethics on outcomes of task (re)allocation and task (re)scheduling

One of the notable outcomes of this project is to make recommendations with regards to the allocation and scheduling of tasks. This dimension was explored in 4 out of 18 interviews, and mainly furthered by the representatives of ACV and ABVV. Although the main rationale of this work package is to outbalance both objective and cognitive physical as well as cognitive load types, as experienced by different operators working on different work stations, the experts received this idea with mixed reactions. Data can be used positively to adjust workloads, assign tasks based on peak performance times, or prevent physical strain.

Yes, so I do see it. Only if you use it in a positive way, you could indeed say, 'Yes, that person experienced stress, and... or should we maybe ...?' Yes, if someone has back pain and certain things need to be carried, then they should handle lighter tasks, while others ... Or if you notice that someone is more resilient in the afternoon, then we schedule difficult meetings in the afternoon. So, there are certainly advantages, but that data can and will likely be applied on a large scale. – LT (ABVV)

Although these 4 interviewees clearly recognise that job rotation enhances *functional flexibility*: provided that multiple employees *are able to* perform different tasks, the first advantage quoted is that it becomes easier to cover absences. Their first remark, however, was that employers must be able to clearly **delineate and consider** the necessary certifications and qualifications required for certain tasks. Increasing the functional flexibility may request employers to train their operators, and in some cases raise debates on working conditions. The second remark, is that the construction of well-being optimisation sounded weird to the interviewees: as if we as researchers would be able to immediately **'optimise people'**, or more particularly operators' feelings and well-being, as if operators are truly manageable assets of an organisation (irrespective of their individual differences). The third remark, is that there is **often resistance**, e.g. mainly elder employees - those who have been performing the same task at the same work station for many year, with the very same colleagues - are attached to it. Even though this scepsis resolves with a minority of operators in the long run (since they then start seeing the advantages such as cognitive challenges and flexibility), the majority of operators deliberately chooses not to rotate both in short as well as in the long run, even despite the potential benefits. This majority tends to see their fixed task pool as a safe haven and remain reluctant to change.

Don't forget that some people do not wish to work in a rotating system. People are quite attached to their tasks, even though they know it is not good for them, because they want to keep doing what they know and can do, as it feels like a kind of safe haven – JVDB (ACV)

Ultimately, the decision on job rotation usually lies with the employer. In case the latter aims to introduce job rotation, there is another set of ethical aspects that should be taken into account: (1) are operators one way or another able to communicate their **interests** or concerns with the organisation, (2) do employees know the root **cause** of their reallocation, (3) what about the **frequency** of reallocating, (4) **how to and who** will decide on the job rotation, (5) relieving the load from one operator is one thing, but **increasing load** (whether cognitive or physical) on another operator is something entirely different: is this something that is ethically agreed upon? (6) Even though we as researchers aim to relieve operators (cognitively and physically), we should be aware that we will hereby **affect their well-being**, if we impose job rotation on them. As such, exchanging a laborious task with high demands and low resources into a cognitively enriching one in itself (so the exchange in itself) may affect operator well-being. Lastly, job rotation systems will quickly refer to function classification systems, the particular job description an operator's job is based on. This function classification comes with **certain expectations w.r.t. working conditions**, also in terms of salary.

So, now operators do have a base salary based on their job classification. That is very clear. They wrote that function. That's their job, and that's your salary. Are we going to categorise your job based on how heavy it is and how much time we need for it. Your task is to place the rims and the tires on the chassis itself. Then, there's a problem: four more bolts are needed, so you step back, pick them up again, and bolt them on. It's done with a reel, which doesn't really change much. You just grab it, and at the moment when time was measured - how much time did Michiel really spend on it? – PVDB (ACV)

Two reflexes, because I'm not good at the others, so automatically, I will be less productive. Does that then affect my evaluation and salary? I have a base salary. It is a job classification. That is very clear; they wrote that function. That's their job, and that's your salary. – LT (ABVV)

2.2.2 Ethics on the use of operator well-being outcomes

It is quintessential to be transparent on the use of operator well-being data. additional challenge is the sensitivity of data-driven evaluations, especially when AI is involved. The accuracy and fairness of these assessments must be verified, often requiring qualitative insights to complement quantitative data. The question discussion revolves around how performance evaluations influence decisions on employee termination. Typically, those with the lowest ratings are most at risk, raising concerns about whether such decisions are made subjectively by employers.

2.2.3 Ethics on the *interpretability* of the well-being outcomes

Two of the respondents came up with the necessity to allow for the ability to have additional in-person conversations triggered by the data or by the operator, to, in the first place help provide potential support for **helping operators interpret data**. Employees may require explanations when monitored parameters indicate issues, ensuring transparency and reducing uncertainty.

Do you always provide people who receive the data with a follow-up conversation to clarify it? Because I can imagine that if something comes up, people might need clarification or further explanation at that moment. For example, if I, as an employee, see a report about myself and certain parameters are not okay, I might need someone to explain it to me. Is there a possibility for this to be built in? And if people have questions or requests, do you share that information with them, or is that not the intention? – PVDB (ACV)

In the second place, provide if necessary **psychological support**. At least one dedicated person in the organisation (trust person, prevention advisor) should be easily accessible for operators to make sure the operator does not feel stigmatised or harmed by the data provided. This is something the organisation proactively needs to take into account. As these two respondents indicate, providing tons, and allowing the operators to check these data based on an operator-centred interface, may still have adversary impacts, and, in case necessary input to contextualise the data is missing, this may once more unintendedly negatively affect operator well-being.

2.2.4 Ethics regarding outcome expectations of well-being measurements

This section revolves around the importance of clarity w.r.t. the expectations on what will eventually change for operators. Five out of all respondents mentioned that operators in essence need a perspective. They should clearly know what the goal of all these measurements eventually is. Firstly, there is a need for a transparency on their influence, do they have the room to mention or address their incentives, to e.g. address complaints in the workplace? If so, this could serve as a lever for operators, as they often find it difficult to raise and address issues without clear guidance and reassurance.

Moreover, when it comes to data collection or sharing information, transparency is crucial. And not only transparency on the collection, processing and returning the data, operators also need to know how their contributions will be used and followed up on, or else they may feel that their efforts are wasted. There's a general frustration when employees share information but see no tangible outcomes or improvements. Essentially, clear expectations and follow-through are necessary to maintain trust and engagement among workers.

There are employees with a lot of complaints, but because then effectively taking the step to address and complain about it and work on it, that is very difficult for them, and they then need a clear framework and clear incentives of 'okay, this is important. We will move forward with this.' It doesn't remain just a dead letter. – LT (ACV)

What else plays into this? If I share something, then I actually really want something to be done with it, and I want to know what is being done with it, that there is transparency.

Because if there is no transparency about it and I don't know what is being done with it, I expect that probably nothing was done with it. And then we've all wasted our time, right? I think there are already many devices. Quite pragmatic in that regard, and that leads to a bit of, and sometimes one big frustration among people. – LT (XSENSE)

All five underlined multiple times that setting expectations time and again, without doing but a single with these expectations loses credibility and trust of the operators. This is what often happens with surveys. One of the interviewees made the comparison with surveys on complaints related to their facility building. In case, you write down your ideas and complaints, and nothing happens in year one, that's still ok. If, in year two, you give the employees the same list with things that could improve, then the employee will try again, and do another effort. However, in year three you lost them. Then, you lost your credibility. They won't think that anything will be changed at all. And that's the downside of conducting services based on surveys: you as a researcher measure all sorts of things, but operators want to see the change.

How you can actually shape things in a more detailed way, rather than the general and vague approaches that make people feel like nothing is being done for them. They keep doing the same things, and over time, they burn out. But this is still often viewed in a very vague way, I think, sometimes. I do have an ideal vision of how it could work in practice. – JVB (ACV)

As can be seen, both practitioners and employee representatives are sceptical about merely measuring without further ado. The ethical question here is, whether or not we can open up the box of Pandora (see below), possibly surfacing tons of well-being related issues, and then leave the company. The last quote of this section nicely underlines that, *measuring* and *knowing* is one thing. But *making a change* is something entirely different. In case we want the operators to have the feeling that we are taking them seriously, we better give them perspective. This of course, lies outside the scope of the project, however, is something we should make the companies aware of.

And yes, what is your role in terms of possible measures, or do you mainly stop measuring? Do we present findings and involve others for that, or do you prefer to reflect at the company level and work out measures yourselves? That's actually a second chapter, because measuring is one thing, but the real work actually begins then, right? –DVC (ABVV)

2.2.5 Ethics on user empowerment versus constrained autonomy

Just as mentioned in the literature, the interviewees stressed on the one hand the opportunity of employee empowerment, and also what can be seen as its counterpart, the risk of constrained autonomy.

2.2.5.1 User empowerment?

When it comes to user empowerment, the interviewees distinguished between two types of empowering operators, the first type of user empowerment is to **receive feedback**, and trans-

parency on health well-being (possibly in relation to production results if employees want this), and that there can be acted upon. The other pathway is that employees are capable of giving themselves feedback on the processes. It could be the case that employees appreciate transparency in their work performance and stress levels. Access to this data allows them to understand their limits and take action, reducing stress. Quintessential then again is that they can truly use this data and act upon the data, not that it is just out there. In other words, and as stressed by researchers at EU OSHA – MC, such methodology is '*not empowering in itself*'. Tools like micro-surveys allow employees to assess their mental and physical well-being easily, promoting self-awareness and empowerment. The accessibility of such data may also mediate the direct feedback of the manager or the prevention advisor. Next quote illustrates that some companies just allow to use a health tool, without further ado.

There are multiple cases in which employers just offer the opportunity to their workers to have such a tool, without any consequence. The worker ultimately chooses him or herself whether or not to use it. It's the employee themselves who, like, if you use a heart rate monitor or something like a Fitbit for your own use, yes, this is the same. The only difference is that it's made available by the employer, which often can do no more than just that. – KDM (VBO)

In some cases, workers in a factory felt empowered when receiving real-time feedback on their performance, allowing them to adjust immediately instead of waiting for end-of-day reports. This transparency alleviated anxiety, as reported by the researcher at EU OSHA.

Sometimes you're not aware that you're too stressed and these boundaries are these stress level really support, but you just don't want to have it in the hand of your of your, of your too high manager. We found another positive example of this in a case study where you know workers receive feedback constantly from the technology and they were happy with that because they could, you know, immediately understand if they were doing well or not instead of waiting the end of the day when the responsible person was, you know, analysing the work done and then preparing a report for next day. – AS (EU OSHA)

The second type of user empowerment is the ability to **provide anonymous feedback** through a digital channel. If this is one of the functionalities of the technology, it encourages employees to report issues or challenges without fear, ensuring they feel heard and can address problems early. The combination of self-reported data with support from managers or advisors ensures that employees not only report but also receive help when needed. This feedback loop enhances their sense of control. The integration of data for post-analysis and ROI tracking helps companies measure the success of well-being initiatives and improve them continuously.

The physiological, so-called objective data is data to quickly say, 'Hey, would you like to report something to the application for yourself, but maybe also for someone who can help you with this?' We notice this or that, and it's starting to show up -can you do something about that? Would you like to say something about it? At that moment, you're actually asking as an application. It could be a notification or something else - can you report an event? At that point, instead of waiting for days, and then having to think, 'I feel like this now' or 'I have pain now,' you can think, 'Well, where did that actually come from?' The quicker you respond, the more accurately you'll understand what's going on. – LT (XSENSE)

All initiatives combined, empowering user or in this case operators, may shift **the power balance** in organisations. In case operators, can base their vision on data, management (according to the Social partner) will surely consider their arguments, their ideas increasingly.

That is an important driver because it forces companies to reflect on their attractiveness, while at the same time, it also gives employees a much stronger position of power relative to their employer, allowing them to say, 'For me, it's not just the salary, but also this and that which are important factors. Or I'm out of here.' – KDM (VBO)

2.2.5.2 Constrained autonomy?

When it comes to the counterpart, i.e. **constrained autonomy**, several observations were made. In the first place, using data as a trigger, may decrease the control operators over their work, in the sense that triggers may show up especially on those moments the operator may experience high levels of cognitive and physical load. At face value, next quote seems to illustrate that self-reporting methods alleviate operators' well-being. However, since the data trigger the action, this could be doubted.

Data is used as a trigger for employees to take action and report concerns early, helping prevent issues from escalating. This self-reporting method empowers workers to have control over their well-being […] And the idea is to say, 'Oh, we just notice that you're experiencing a peak in stress.' Or we now recommend, for example, to go exercise later to reduce stress levels, or to do this or that. A few recommendations, and maybe you'd like to say something about that? – LT (XSENSE)

In the second place, continuously generating data may essentially create more stress rather than helping, since the operator may have the feeling continuously being checked and surveilled. In the third place, a concern raises that replacing employees' decision making with devices or sensors could undermine their ability to think critically and take responsibility for their own well-being. Essentially, data may provide advice and guidance, still overly relying on technology for decisions could limit employees' autonomy and their capacity to manage their own health and safety independently. This was also a worry raised by ABVV and ACV representatives. They more particularly emphasised being worried that the new method of measuring would cover the entire

Data-driven systems should ideally empower workers to take control of their well-being (e.g., through self-reporting mechanisms), but when used incorrectly, they can undermine workers' ability to make decisions for themselves, creating a feeling of being watched or controlled (Big Brother effect). Employees may also feel pressured to comply with recommendations without critical reflection on their personal situation. – JM (ZSENSE)

2.2.6 Ethics on data sharing and transparency

Importantly, 1 practitioner argued that not all data is the same. And that operators overall are more willing to share physical data than mental health data, as privacy and anonymity play a larger role in mental well-being. Some see mental health tracking as more of a private thing rather than something to be openly shared. This practitioner added that operators want **control over who sees their data**. Genuinely, operators are not this hesitant to sharing data, provided that they can decided themselves who will be seeing their data (one) and that some actions are taken upon their data that favour them (two).

Employees must be given the option to **control which data** they share, with the ability to modify privacy settings. Employers and employees need clear agreements on what data can be shared and who can access it, with the option to keep certain data private. A practitioner argued that the main challenge they faced was allowing people to choose who they share their data with and whether they want to share it at all. They have made progress in this area. They decided to separate personal data from company data, which allows for more transparency and control. This creates two distinct categories: personal data linked to the individual and company data related to work, jobs, and locations.

Key considerations include deciding which data to share, how to share it, and ensuring that privacy is maintained. For example, data can be private for those outside the relevant job roles, like health and safety advisors. There should be flexibility in managing privacy settings, such as defining what is shared publicly, anonymously, or privately, and giving users control over these settings for each report.

Operators are generally open to speaking with someone about their work-related concerns but prefer a **trusted person**, this is someone who is not always from within the company, preferring to share it selectively with a prevention advisor or a trusted colleague.

To speak with someone? But it must be a trusted person? And that is not always someone from the company. They do not always feel equally comfortable with that, yes. Okay. I do want to keep it. I might want to share it specifically with a prevention advisor or a colleague or a colleague and the prevention advisors, so that there are combinations that are possible. I don't know how to deal with it, you know? If they always come out badly in the data ... Maybe they would then want to withdraw and not want to share their data anymore. It could lead to comparisons between different employees, where it's said, 'Well, that person doesn't have an issue with it, and you do?' – KD (YSENSE)

2.2.7 Ethics on datafication and reification of well-being data

This section addresses concerns about the **datafication and the reification**. Essentially, this means that operators risk to be treated only through or by means of the data, which in turn, may have implications for their well-being. In what follows, we highlight the risks of turning employees into data points, where their work and personal health data are used, which may affect their autonomy and privacy.

The first two quotes are about the measurability of well-being indicators, and more particularly, the main drivers organisations have to do so. The first quote indicates that *measuring is knowing*, however, the sidenote is made that quantifying and objectifying well-being **may distract** the attention from what is really at stake. However, there is scepticism, as these systems may not be as impartial as they appear. For instance, systems that track workers' well-being may, just as productivity data, become problematic if a worker does not fit the 'average' profile. There's a concern that data systems, while intended to improve efficiency, can lead to new standards that have been **data-driven and data-imposed**, which drifts away from personal interpretations and not might not account for individual variations.

It feels as if the well-being outcomes are reduced to measurable indicators, however, it will just be one indication of objective or subjective well-being: this may distract the attention from what really matters, i.e. – not only work station, worker, outcome relationship, but there is much more at stake, e.g. other work conditions and relationships also play a major role. A holistic approach is needed. – KDM (VBO)

Some say this is more 'objective' as everything can be recorded with data. The number of errors you make can be objectified, as well as the speed at which you work. It moves away from personal relationships - the smaller the gap, the less leniency, the larger ... systems allow this, but if it's not fast enough, people will be waiting to take your place. – RH (VUB)

Following two quotes illustrate that the **distinction between data**, personal data and production is becoming increasingly vague. As such, productivity data may be interpreted as well-being data, and vice versa, well-being data may be interpreted as productivity data, as illustrated in an interview with ACV representative JVD. This is also nicely underlined by Researcher lawyer DG:

Distinguishing between personal data and production data quickly become outdated. The line between monitoring and surveillance is thin, especially when it comes to product quality and responsibility. Sometimes, HR departments might get involved with employee well-being, perhaps even developing apps to track how employees feel. Shockingly, very few people have issues with this. However, temporary workers may feel stigmatised if they don't fit the 'ideal worker' mold, which can undermine team productivity. In academia, for instance, the average burnout rate is around six years, reflecting the pressure on workers. – DG (UGENT, HIVA)

Especially because the distinction becomes vague, this researcher argues the importance of **data minimisation** in the workplace. He suggests that while monitoring employees' activities is sometimes necessary for safety, companies must be careful not to collect excessive personal data. Employers must also recognise that they are responsible the costs (mental or physical) associated with maintaining a secure and ethical workplace, balancing privacy with the need to monitor and ensure employees' safety.

Another thing is the inclination to overly focus on individualised data, instead of seeing well-being at work as a collective event. The risk is that as an outcome employers may be **individualising** the event of well-being at work, far more than seeing it at the collective level. The perverse consequences thereof is **internalised responsibility**, or, as nicely shown in the literature, that operators will be inclined to see themselves responsible for their own data, i.e. their own well-being, instead of their employer. Having tons of individual data runs into the risk of not zooming out to the collective level.

Some worry that monitoring systems focus too much on individuals rather than fostering a collective approach to health and productivity in the workplace. Individualisation of issues. We can still add and improve things, so in that regard, I think it's good, with a few caveats from our side, of course. It should not be used individually, but rather collectively. – LT (ABVV)

The fact that a device or a sensor is put instead of this code decisional kind of Co governing the workplace and improvement is putting away this prevention obligation from work from workers and from companies and workers, and pushing away that critical thinking. – AP (ETUI)

When work and maybe even well-being is measured by **output metrics**, employees can feel that they are reduced to numbers rather than valued for their skills or contributions. Instead of making sure work is done properly, one interviewee argued that they may be too focused on their well-being metrics as an extrinsic motivator, which may negatively impact their **work ethic** and sense of purpose, leading to an extra stressor. The pressure to perform based on such data can strip employees of their agency and autonomy. In another interview, there is a discussion about monitoring systems in workplaces, where workers may adapt to the work system due to self-imposed gamification, adjusting their work habits and work behaviour to remain within acceptable productivity or quality levels, sometimes viewing the system as a gamified challenge rather than an obligation. The issue presented in the quote below may be interpreted as well for well-being data.

And there are people who are working with their heads bent over the screen, visible to everyone, where there is a point or a bar indicator. Still, that young one plays the game again and they have such a line, the waterline, and then it's a bar above, and as soon as the production drops or the quality drops. And people didn't have any problems with that because they saw it as a computer game against themselves and they saw it as a challenge to do just enough, not too much, but still enough to stay in the green or above the waterline. And that is the case with Ontex, they have a number of companies. If we could just see that live, that would really be worth it. – JVB (ACV)

We conclude this section by shared worry expressed by 2 employee representatives, who are inclined to presume that such technological methodologies, in the long run at least, will not be used to **complement ongoing well-being measurements** but instead replace existing methods. The interviewees expressed that the technological methodology would ideally be used as a complement to existing practices aiming to fortify or improve operator well-being rather than as a replacement of preventive initiatives. Here, there is a worry among all employee representatives interviewed. There is some concern that these technologies might be misused or create unrealistic expectations. It is important that the use of technology is clear and collective, not individual, and that it doesn't lead to disappointment if the outcomes are not immediately transformative. Proper framing and communication are key to managing expectations and ensuring successful integration.

It should be able to better map or monitor certain things that are not happening today. But I see it more as a supplement rather than a replacement, and we are often a bit afraid of that, like, but isn't this new technology going to be used to replace meetings? – LT (ABVV)

The challenge of balancing personal health information with performance standards is mentioned, with concerns that focusing solely on data could overlook the human aspects of well-being and health – PVDB (ACV)

2.2.8 Ethics on data-imposed normalisation and data-facilitated harm

This section emphasises that datafication and reification of operator data, may run into the risk of creating new norms in the first place, and inducing data-facilitated harm in the second place. It shows concerns about how data set new norms and how data might be used to make decisions that harm employees, increase stress, or lead to unfair treatment.

2.2.8.1 Data-imposed normalisation

The first two quotes indicate that data may impose **normalisation**, yes, and that these data may lead us towards averaging well-being for operators, leading to **data-profiling**. This means the technological methodology will work properly for those operators that are average w.r.t. their individual characteristics, e.g. weight, height, HRV, etc.

We create new norms before you know it: at that station, data must be anonymised. You'll notice fewer health issues, a bit of shuffling in the hall, and then we'll intervene, seeing a decrease in social problems. What will we do? Yes, we'll intervene, and it will decrease until it's acceptable, but this could have potential negative consequences elsewhere. – ACV representative JVD

Take the example of tasks, calculated by averages, which works if you are the average person. But once you fall to the left of the curve, you'll be slower; you must meet the standards. If you're not performing well enough... – Research expert

2.2.8.2 Data-facilitated harm

Data-imposed normalisation may lead to data-facilitated harm. This is to be especially careful for, since data-facilitated harm may slip into the system unconsciously, and may have severe consequences for the operators in situ. The bulk of the interview quotes are not so much about the normalisation, but about the automated decision making or the managerial decision making based on workers well-being conditions. There are potential negative consequences of data collection, such as creating new, stricter standards that could harm workers. The need for careful handling of well-being data is emphasised multiple times, with an acknowledgment that interventions based on data can have **unintended consequences**.

Firstly, there's a risk that people might become scared. If they don't score well in evaluations, it could signal the end of their job. This creates a clear risk, and employees might feel more anxious and **insecure about their job**.

Employees may fear that poor scores on health or performance metrics could result in losing their jobs, leading to anxiety and stress. – EP (ACV)

There is a concern that **data-based profiling** could lead to **discrimination** or unfair treatment of employees, particularly if conclusions are drawn from certain datasets that may harm workers' chances, such as if data is misinterpreted or if employees are disadvantaged due to factors like stress levels or health status. Ethical frameworks must be in place to ensure that this data is not misused.

Maybe they are heavier or of a different origin, so that it doesn't turn out to be to their disadvantage. This is something important to consider when drawing conclusions based on data. But this is also partly the ethical framework, so it must be properly assessed. That people are advantaged or disadvantaged because of that data, where they might have less control over it. I think that's a risk. – OS (ALAW)

The technology worked better for people with lighter skin colour, as it required more charging for people with darker skin colour, which caused less accurate results. This led to a decrease in use among the latter. – RH (VUB)

One of the additional issues here is, that it sometimes comes to individual differences. For some people stress reactions will not show up that early in the data, whereas their subjective feeling may indicate high rates of stress. The other way around, others may have high stress reactions in the data, whereas these employees don't feel stressed at all.

Some employees handle stress well and perform better under pressure, while others struggle. Understanding these differences is crucial for well-being initiatives. Additionally, one could wonder whether such comparison arises between different employees, where it's said, 'Well, that person apparently has no issue with it, and you do?' – OS (ALAW)

Another thing is that the work-related cognitive and/or physical load indicators may affect the allocation and scheduling of operators differently. Whereas people may have signed a contract for the same job (same salary) – characterised by similar load types, changing these load types across people may seem optimal from managerial perspective but, in the view of operators not ethical. For instance, the reasoning that (accidently) being a person with an above-average height and above-average strength, may not necessarily lead to above-average exposure to physically harmful tasks. From the overall perspective of 'optimising well-being' for the entire workforce of an organisation this makes sense, but all operators' position may improve, only provided that the situation of some operators decreases, and exactly there lies the problem.

If someone is more sensitive or weaker, certain proposals might be made to increase their workload because you know that the person is less resilient at that moment and might accept something they wouldn't normally accept in a regular situation. For example, their own contract extension might be brought up, because you know they probably won't push as hard for a salary increase or something like that. So, it could potentially be misused or be misjudged because of this. – EP (ACV)

This type of data-based profiling and the data-facilitated harm that stems from it, is thought to also affect the **recruitment and retention policies** of companies in the long-run. The hoped for outcomes may essentially affect the selection and recruitment of new operators.

An employer might prefer employees who are in perfect health - who have no back issues, no stress, and are as healthy as possible to ensure high productivity. But personal data could be misused to screen employees, with certain individuals being deemed 'unsuitable' or 'unfit' based on that data. This could result in employees being unfairly dismissed or discriminated against. – JVC (ABVV)

There is a risk that subjective judgments from employers may influence decisions, like choosing to let go of employees based on personal traits (e.g., high stress levels or smoking), even if their performance is adequate. – JVB (ACV)

Next passage interestingly delves a bit deeper into the attitude of an interviewed practitioner w.r.t. **internalised responsibility**. My question to this person was very broad - could such a system unintentionally lead to attracting, recruiting or hiring especially super-healthy, highly motivated, and engaged employees? The answer of this person was as follows:

Yes, yes, and is that a problem? That's the question. It could be that people who... we know smoking isn't healthy, but smoking has a huge impact on the average heart rate or faster stress reactions. So, the question is, how far do we go? I also follow you, and I heard you mention in the meeting that you want a totally integrated system where... maybe in 10 or 20 years, the data we gather in the workplace could be forwarded to or presented to a doctor. I heard you say that, health systems, and I'm a fan of that too, but I also wonder, will it be stigmatising to, for example, those two people who might be in that one team, like I just mentioned as an example? Won't people sympathise with

them? Does this turn into lifestyle unitarist, where it's implied that their lives are being judged, so that's a bit of the question – LT (XSENSE)

Hereby, we underline to overview the ethical view of the practitioners and the developers of such measurement technologies. Their position on the ethical side of the technology (their view, but also what they miss) will have consequences in practice. In terms of recruitment and retention, or laying off, we also run into **legal issues**:

I don't know legally if we can actually terminate someone after an evaluation, where someone needs to be let go. If you're making an evaluation, you'll probably pick the person who's been assessed. It might be a subjective decision from the employer regarding that person. If the person is considered the least valuable, it could be based on objective data, but it could raise legal issues. There's a chance that, for example, in any company, someone with a higher stress level - who may otherwise function well - could be disadvantaged because they smoke or have a naturally higher heart rate. – OS (ALAW)

More so, workers and unions are concerned about personal data being collected, datafied and **used abusively.** And that there is often collected beyond what is strictly necessary for managing health or workplace safety. This can lead to unfair evaluations, especially if the data is used for purposes other than what it was initially intended for. There's a fear that companies could misuse personal health data to screen out less 'ideal' workers, such as those with chronic health issues or higher stress levels. In essence, while data can be used to improve workplace productivity, the ethical implications, privacy concerns, and potential misuse of personal data remain significant challenges.

The concern among workers, especially from trade unions, is the potential abuse of collecting and using personal data. They worry that data might be collected in ways that go beyond what's necessary for management or occupational safety and health protection. This issue is related to important psychosocial risks. – MC (EU OSHA)

A final general remark is: what is the added value of these data-based conclusions that will be drawn, and if there is any. The question then is, how organisations and which parties therein, will be using these organisation health and safety data (intendedly or unintendedly) and, whether they will be using it in the domain of preventive policies, or only as a way to react to issues? The question whether these technologies can be misused and be interpreted as means to gains productivity gains needs to be seriously debated.

2.3 Ethics and the balance of unitarist and pluralist interests at work

2.3.1 Managerial surveillance versus workplace monitoring

To start with, four interviewees emphasised distinguishing between **surveillance and monitoring**. They negatively connotated surveillance is often associated with punishment and control, while monitoring is not only associated with negative aspects. However, constant monitoring can still create stress and negatively affect worker health. Sometimes the line is thin, and is it hard to delineate these two, since there is also a subjective component to whether or not employees are surveilled vs. monitored. The **right to do surveillance** is certainly a thing.

As an employee, the core of your labour contract is that you sell labour in exchange for wages. But in addition, and this part is sometimes forgotten, you are also selling your independence a bit. You are essentially bound to an employer. It has always been this way - you sell labour in exchange for wages, and for your independence. You submit to the authority of the employer. Labour is provided, so it must be worth the money, meaning the employer has the right to measure it … Think of the times of Daens. At the end of the 20th century, people had to have their work books with them, this was their personal data. Workers had to have their own data with them. You had to carry it with you, your own data, and could be controlled, there was supervision in person, surveillance if you want, but it was transparent. It's all about to what extent you do this. Yes, yes, to what extent can an employer, who indeed exercises authority over his employees, also monitor them in a certain sense? You had to really monitor employees to the point where their private life, which they also have at the workplace, is also involved. Only that the employer comes into contact with that, right? – DG (UGENT)

The question is ,however, how and where in the organisation does the data needs to circulate. Originally, the surveillance should be allowed to the **extent the data is part of the production area**, for instance, a line manager has to have data on ongoing processes of his employees so as to act. In case (and only in case) the data is required to keep processes running, the data can be shared. Possessing certain data, may be part of this person's job. The question however, is whether it is ethical to aggregate these data (even after anonymisation) to higher levels within the organisation.

Especially when it is about tracking systems in the company. But today, much more the systems where everyone is sometimes tracked from minute to minute, second to second, what he or she does. – JVD (ACV)

Excessively monitoring may have psychological impact. Surveillance tools, even when justified and when legal, may create a *Big Brother* atmosphere, leading to worker stress and anxiety and may unfavourably affect well-being. As an example, the constant collection of physiological or survey data might seem intrusive, even if the intention is to improve well-being. Workers may feel uncomfortable with such invasive surveillance and may become frustrated or demotivated.

An important issue is that surveillance tools are nowadays often used to monitor workers, and that, organisations are not aware of GDPR and AI act regulations, in particular and with regards to this project, those regulations that protect employees' health data. What we do see here, are quite some sectoral differences when it comes to surveillance habits. Examples include factory settings where workers were monitored by supervisors, with an understanding of when they were being watched. There was also mention of monitoring systems used in industries like food production or logistics, where the data collected is used for operational improvements, but still raises privacy concerns. In such cases, surveillance has proved to be essential to keep track of the processes, however, in those cases is has also been misused in particular cases, since often (cameras) more is registered than necessarily required. This is something to be aware of.

But, yes, naturally, this leads to an interesting discussion, can you, as an employer, do something with the consent of your employee who is in a subordinate relationship? Only the way in which privacy is interfered with for an employee depends on the company and sector. Right? So, because life ... It feels right, and those who see it, only see it, but that's all a bit mixed with surveillance or other things. Naturally, that was not intended to be, and both parties share the principle of it as well. – MC (EU OSHA)

Research expert RH mentioned the concept of **sousveillance** as the individual recording of an activity by an employee. W.r.t. sousveillance, it would not be the person in the hierarchy of the organisation that excesses control, but rather the user (operator) him or herself. He or she would continuously check him or herself, leading to excessive disciplining, as also mentioned by philosopher Foucault. For workplaces, this may cause operators to continuously check their own health status, possibly improving their health, but also inducing responsibility for their own data.

This part on surveillance and monitoring illustrated that there is difference between monitoring and surveillance. What seems to be quintessential is **transparency** on what data is collected, and what these data can be used for, just as in the historical example: here the line manager had the right to measure the progress, and so to say, surveil the status of the production process and the work delivered. However, the worker in particular was always aware of the surveillance. If not, the operator may have a continuous feeling of the panopticon, feeling under continuous pressure with the adversary effects on his or her well-being as a consequence. The legal aspects will be overviewed in below.

2.3.2 Managerial responsibilities in relation to worker well-being

Five of the interviewees pointed to the **responsibility of management.** In the first place the responsibility management bears to take preventive actions to guarantee workplace well-being, but also in the second place the responsibility to be transparent and legal when it comes to employee rights. They must use data responsibly, ensure compliance with legal standards, and address any issues that arise promptly and ethically.

To start with, ETUI research expert claims that the legislation on well-being uses the intention of the employer to ameliorate the well-being of all employees, and take preventive measures as a cornerstone. I think you will need to make that clearer today. As you just mentioned, the employer is responsible for the well-being policy within the company.

Well, they are responsible for taking preventive actions and preventive policies that are expressly designed to prevent psychosocial hazards or physical asset accidents? And to prevent risks and to increase uh health.

A second point is that employers are **liable** when making agreements or contracts. Thereby, the employer is also responsible for the complexity of decision making in the workplace, particularly when relying on technology like sensors. He points out that employers may mistakenly believe that these tools are foolproof, but questions whether they should be used to make significant decisions about employees' well-being (e.g., health or safety), especially when the reliability of such systems is uncertain. Employers must also agree to ensure that there is no misconduct or misuse. This responsibility also includes providing regular feedback to organisational structures (e.g., employee councils) to maintain compliance with rules and ensure fairness. The employer must also ensure that personal data is not misused and that privacy rights are respected.

The employers need to ensure they are adequately protected and accountable for their actions in the workplace. In particular, this responsibility extends to the ethical and legal obligations they have towards their employees. – OS (ALAW)

In my opinion, it is the responsibility of the employer to draw the right conclusions based on the data: and that the employer acts properly and promptly upon the conclusions. – LT (XSENSE)

A third point, relatedly, addresses that employers should be aware of the increasing stress levels in their workforce and take **appropriate action to prevent harm**. He argues that employers have a duty to protect their employees, even when handling sensitive data, and that neglecting known problems is a violation of this responsibility. This interviewee argues that what has been missing in the literature and as a topic of the interview is the responsibility managers bear to act upon their knowledge.

Yes, what you're still missing is- how shall we call it – 'measuring is knowing', right? By measuring how bad the well-being of your colleagues and employees is, the greater the responsibility becomes to do something about it. – RH (VUB)

At this moment, we do not have actionable well-being metrics. And these data on well-being are mostly covertly discussed (at most once a year with manager and worker individually).

'We know now individually that there is an issue when it comes to well-being at work', this interviewee argues, 'but luckily, we don't have enough data, I think. Otherwise, we would have had to take much more responsibility for it already.

To this interviewee, the manager bears the responsibility to act upon data w.r.t. well-being. In his wording, the data could (or should) serve as a **signal function** that you cannot simply ignore. More so, in his opinion releasing tons of data may bring to the surface way more issues that the

employee nor the employer were beforehand aware of. In that sense, implementing such a technological methodology may feel like opening up the **box of Pandora**. However, what you can say is that the results or recommendations can be taken further and that, in the future, there should be consideration of how employees can better highlight certain obstacles.

I am really curious to see how employers will react when these issues come to light - especially considering all the additional challenges they will have to address on top of the existing privacy concerns. I don't think the employer will enter into specific arrangements or additional commitments with you based on the findings of that research. – MV (UGENT)

2.3.3 Social dialogue

The main focus of social dialogue in the workplace revolves around improving work conditions, ensuring control, and promoting equity. While topics such as employee well-being, psychosocial health, and ergonomic issues musculoskeletal are gaining more and more attention, it needs to be mentioned that the expertise and knowledge required to address these concerns effectively is sometimes lacking. And in addition, most of the discussions are still about the less soft, and more classical points of discussion, e.g. wage bargaining and other working conditions. When it comes to well-being at work, the responsibility often falls on prevention advisors, but as said, there is still **less focus on 'soft' themes** like psychosocial health and well-being compared to traditional issues.

Yes, with the classic themes, I would say, it's mainly about salary and working conditions, and less so, yes. When we talk about the so-called 'softer' themes - although I do think there is growing interest, especially in our psychosocial well-being. – EP (ACV)

In several interviews, it has been emphasised to not solely focus on the individual operators when it comes to participation and consent, but also be aware about the **broader collective** and organisational perspectives. In addition to the individual operators, it is the entire organisation that should consent this idea.

So, certainly, also to the trade unions and such, and also to the idea that it should not be too focused on the individual. Yes, we are indeed aware of this, right? It's not just about the individual, but also about the tasks and the collective, and the interaction that needs to be stimulated there. And don't forget, it's not just the individual, especially from our regulations and connections. So, it also involves the collective, the hierarchical line, or the employer, not just focusing on the individual. We're going to address this together. – DVC (FOD WASO)

There is a concern about the balance between privacy, technological tools, and workers' rights, with a need for clear communication and agreement on boundaries. The role of trade unions is crucial in ensuring the protection of workers' rights, but their involvement may be hindered by a

lack of awareness and literacy, particularly regarding data privacy and the implications of new technologies like wearables and surveillance systems.

And I just think, no, they often also think like this: Let's involve the unions as little as possible when it comes to anything related to privacy, so that companies can handle everything on their own. But, of course, this doesn't lead to any interesting discussions. Can an employer really do something with the consent of an employee who is in a subordinate position? […] And I think sometimes it also comes down to union power dynamics. Of course, if my company says, 'You have to do this,' the unions can say, 'If you don't, we'll call a strike,' and then the employer will back down. Naturally, in some other industries, that's less obvious or the power dynamics are different, so that certainly plays a role. – PVDB (ACV)

Even despite their lack of awareness and their lack of data literacy, one of the interviewees argues that employee representatives may be eager to be part of this project, in particular because they want **to enforce measures** they can use against employers to outbalance them in a conflict.

Trade unions also say, we want to enforce an even stronger enforceable framework, where they actually want to have harsher measures to use against employers when they are not given a say. The question is, what is the way forward? Because employers sometimes no longer want to talk to trade unions, simply because the discussions have become so sharp and legally oriented. – RH (VUB)

Well, I think you can make a distinction between companies with social dialogue and committees and companies without social dialogue bodies, right? And in companies with social dialogue, I would definitely involve the CPBW (Committee for Prevention and Protection at Work) alongside the management. Why? Because the CPBW is the effectively elected worker representation that sits there. […] Of course, in smaller companies or those without dialogue bodies, I think it's mainly the management, the prevention advisor, and then the operators or the workers themselves who would provide issues or feedback based on their expertise. - DVC (ABVV)

Even though the large majority of the people interviewed strongly favour to integrate the social partners and the unions, some interviewees argue that the unions may unnecessarily be harsh on the project, and **delay progress**. And not for the better of the employees.

The passing party to management and management to the union. Unfortunately, the issue is often made worse instead of being improved to bring people together. Again, direct dialogue between the worker and literally the CEO of a large company is often better, I think. Rather than involving a union, which might just make it more complicated, people sometimes just want to defend their rights. In fact, it's one of the things that also hinders us as a company from growing with those well-being applications. Because we really need to build those other applications as well. Employers sometimes say very literally to me, 'Yes, but if I start this, I'll open Pandora's box,' someone literally said that. On the other hand, not recording anything is, in my opinion, not an

option for the employer either. But many employers are still unaware, or not conscious of the legislation. – LT (XSENSE)

Just as there has been scepsis on the role of the manager, and his or her potential to either intendedly or unintendedly affect employees by means of collecting and analysing tons of data, the following quote illustrates scepticism towards the employees, who themselves may misuse or manipulate the data.

Yes, alleged abuse, and also the idea that employees are lying. There is also fear of employees. This is another form of abuse, not just the later lies. They say, 'I didn't do anything,' but also simply lying about what happened to make an excuse for receiving benefits and staying home. – EP (ABVV)

A much debate issue when it comes to social dialogue has been the discussion on **transparency of the data** among both employer and employee representatives. Both the ACV and the ABVV representatives recognised that management is not always solemn, sometimes hides behind the GPDR legislation so as not to inform the employee representatives.

They have all that data available. They also need to collect it. They also need to pass it on to external services, for example, when it comes to health monitoring or something like that. So, that data is there, right? That's what I meant earlier. It has become a difficult issue to still handle in a constructive way within a consultative body. You are sometimes confronted with employers who hide behind privacy to avoid sharing certain information. Additionally, it means that we are dealing with many issues. – LT (ACV)

The employee representatives feel that the lack of transparency and **withholding of data hampers their ability to defend workers' rights**. There's also a fear that certain data releases may lead to negative consequences, such as legal issues or complications in employee relations. Employers on the other hand, are also wary of sharing too much data, fearing that it may lead to legal risks or misuse, particularly with privacy violations. This fear, combined with mistrust of unions, creates a barrier to effective collaboration and limits progress in certain workplace initiatives, especially those related to worker well-being.

The argument then is to stop sharing or providing certain information, which limits their effectiveness at that moment. When exchanging with each other, if you always get the answer 'there's a problem,' then you're not progressing, of course, right? I understand, of course. Privacy is important, don't get me wrong, I'm not saying we have something against it, but it can sometimes be an obstacle. I'm not saying this applies everywhere, but it is a reality. This happens or occurs on certain days. But it's already been shown in the past that, for example, our representatives no longer receive the list of names. For example, JPR considerations, while for the committee, it's required that they give their advice or approval on certain matters. And then, at that moment, they can no longer or insufficiently fulfil their role. LT (ABVV)

As can be seen, the relationship between employers and unions can be strained, especially when data privacy issues complicate negotiations and dialogue. This may indeed result in distrust:

> **Because they actually don't trust their own unions, and the union trust doesn't work for them, so that's a problem, often the sacrificial role towards each other. It's a pity, and it really gets in the way of progress here. And then the other point you mentioned. – JVB (ACV)**

The practitioner interviewed LT (XSENSE) argued that this dialogue standstill also hinders his company to grow in developing well-being applications. Because we really need to build those other applications as well.

> **Employers sometimes say very literally to me, 'Yes, but if I start this, I'll open Pandora's box,' someone literally said that. On the other hand, not recording anything is, in my opinion, not an option for the employer either. But many employers are still unaware, or not conscious of the legislation.**

To conclude the section on social dialogue, we mention that two representatives presume that the employer is hesitant to share data, out of **fear to be law suited**.

2.4 Legal framework(s)

As authors we are not legal experts and therefore do not aim to provide a comprehensive legal analysis of the regulations concerning the ethical, privacy, and practical aspects of employee well-being measurements. Nonetheless, it is important to have a clear understanding of the relevant legislation.

2.4.1 When ethics meets law

Besides the question of what is legally possible, we first point out four aspects that deserve to be addressed before digging into the legal aspects.

2.4.1.1 Distinguish what is legally possible from what is ethically desirable

In the first place, we must not forget to question the **desirability**. This question is one we too often and to easily overlook. Just because something is legal does not necessarily mean it is desirable, that's correct. In addition to asking what is legally possible, or even prior to what is legally possible, we must question the desirability. Just because there is a framework for data does not mean its use is desirable. The context matters - such as the workplace, the sector, the product - but also how the data is collected and what happens with it.

2.4.1.2 Move beyond the absolute minimum criteria

In the second place and in addition to the desirability and legality, employers and employees should be aware that what is legal refers to an absolute minimum. Properly implementing this technologi-

cal methodology would mean to **move beyond the law**. In fact, fully complying with any legislative framework, in the broadest sense, is something companies can do perfectly. However, this does not guarantee the result aimed for will be reached, right? Fully complying with well-being legislation and data protection legislation thereby not necessarily means high rates of employee well-being are necessarily guaranteed. In that sense, complying with legislation is a necessary condition, but not a sufficient condition. Companies that are taking part in this project should distinguish between reaching the goal of a legislative framework - which is still about setting minimum requirements - and the fact that you are not always required to shape, develop, or mold it further. A legislative framework will never help with that - you will have to build that yourself. So, legislation sets the lower boundary, but shaping it into something meaningful and developing it to achieve your intended goals - that is up to you. The employer representative argues here that companies aim to raise for standards that are above minimum requirements imposed by law:

What I think is important from a business perspective is a level playing field - whatever its value may be. What we actually mean by that is having a basic set of rules, legal rules that everyone respects, in order to filter out freeriders and cowboys. – Employer representative, KDM

2.4.1.3 A stakeholder-based approach stretching the technology timeline

A third thing is that we ethically aim for a **stakeholder-based approach** and to expose the interests of various parties across the technology design and technology implementation phase. This aligns with the idea of social dialogue, much valued here in Belgium, but we see, however, that this doesn't happen often.

2.4.1.4 Necessary preconditions: digital literacy and digital awareness

Before stepping into the legal part, a fourth thing to mention is that there are two necessary preconditions that precede each part of our law system: (1) any subject should be informed about the law, and (2) any subject should know what the repercussions are of (not) following the law. For the purpose of our project, it seems quintessential to consider certain personal data as operators' property and handle it accordingly. In the first place, operators should be fully aware of what they are doing: one of the fundamental principles of any legal system is literacy, ignorance of the law is not an excuse. You were informed but misunderstood it completely. Thus there is **data literacy**: you must understand what data is, which data is being generated and released. And secondly, there is **data awareness** - you must understand the consequences of sharing data. These are the two key aspects: understanding what data is and how it is processed. understanding the consequences of data disclosure.

2.5 Legislation: different types at different levels

To start with, the part on the legal dimension is one that has multiple layers covering multiple branches of the law come together, being (1) legislation on quality of work and prevention and protection legislation, (2) legislation on data protection legislation, (3) legislation on the implementation of new technology at work,. Main lesson here stressed is that even within one and the same branch of law, we sometimes have grey or even conflicting zones. Before continuing, the proposal

of our technological methodology was presented to three lawyers as part of this task, and all three argued that **within the context of our project**, especially since it has already passed the ethical committee, is ethically and legally approved.

When it comes to (a) law on quality of work and prevention and protection legislation, we rely on **worker protection legislation.** These laws act at national and EU level and detail law around health and safety that are mainly based on the principle of prevention, requiring collaboration between employers and employees and their representatives. Law is at least health and safety law at work and will be law in Belgium and in the EU is based on general principles, one of which is prevention and the prevention principle. It's really a human activity in which workers and employers have to come together, discuss about the risks, do a risk assessment conjointly and think about the possible measures to eradicate or mitigate the risk. Interestingly, employee representatives here refer that the introduction of devices and sensor-based measures may over time serve or being used as alternatives to collaborative decision making, which may eventually undermines the prevention principle and critical thinking necessary to mitigate risks. This worry was shared among two employee representatives. Being overly confident and relying on data, may drive away the attention from what really matters.

The lawyer and employee representative ACV mentioned that often legal discussion arise when someone is fired because the '*employer accidently stumbled on something*', when eventually it seems the data were gathered by means of an illegally placed camera, or that they for instance found all sorts of data by means of unintended use of ICT systems.

When it comes to (b) law on data protection legislation and (c) law on implementing new technologies at work, we make divide splitting up the legislation at several levels.

First there is the **employee level**: employers and third parties need a valid legal basis to process personal data. Personal data e.g. requires explicit consent. Issues here may be that (1) most employees are not highly sensitive to data privacy issues, but some are; (2) the employer always as well as the third parties have the information obligation; (3) asking employees for consent is difficult due to the hierarchical relationship with employers, making truly voluntary consent questionable (Lawyer, OS). There is a debate on whether processing of data (data processing agreement!) can rely on legitimate interest, but in many cases, consent seems necessary.

Second, there is the **company level**: employers decide on implementing new technology, followed by formal consultation with worker representatives. Here the legislation refers to CAO 39 the introduction of new technology triggers a formal *consultation* process. Even if laws and ethical frameworks exist, companies struggle to apply them due to lack of knowledge or resources.

Also at the third level, the **sectoral level**, outdated regulations based in sectoral agreements on data protection and surveillance are found, stemming from the 1980s require updating. Attempts to renew national agreements (e.g., Collective Labor Agreement on technology use) face resistance from employers.

At the **national level**, Belgium has privacy and data protection laws but lags in enforcement and adaptation to modern challenges. Belgian Data Protection Authority (DPA) has issues on actualising recommendations but faces limitations in enforcing privacy in the workplace. Practitioners often refer to France's CNIL and the Dutch Autoriteit Persoonsgegevens since these are more proactive

in issuing guidance. Data Protection Authority has issued recommendations to limit unnecessary (data minimisation) data collection and worker surveillance.

At the **EU level**, we now have the GDPR, which restricts excessive data collection and certain types of processing (e.g., health and well-being data), we have the AI Act restricting e.g. AI tools that measure emotions (e.g., facial recognition for mood analysis) are prohibited. We have the Occupational Safety and Health (OSH) Framework saying that employers must ensure proper information-sharing with employees regarding workplace data use. We have the European Framework on Digitisation, promoting a process based approach towards new technologies at work and limiting data collection and analysis. European regulations are a mix of data protection (GDPR), AI governance (AI Act), and worker protection (OSH), and more framework create a complex legal landscape.

Yes, yes, there are pieces of legislation that receive more focus or attention, which may sometimes divert attention from other frameworks. We will probably see the same thing happen with the AI Act, right? We now see that GDPR is getting most of the attention. Right now, it is a hot topic, but once it officially comes into effect in two years, we will likely witness a similar shift. Indeed, there will be a transition toward a stricter legal approach, and that will have to be evaluated accordingly. – PVDB (ACV)

2.5.1 Anonymisation and pseudonymisation

We should be aware to distinguish anonymisation from pseudonymisation. **Anonymisation** refers to the process where data is completely detached from individuals, making it impossible to trace back to specific persons. When data is anonymised, it is no longer considered personal data under privacy laws like GDPR. With truly anonymised data, one can do much especially compared to pseudonymised data.

An employer representative interviewed mentions that employer are always so eager for data, but stresses that they themselves do not so much with the data themselves. The aggregated data do not help to pinpoint the issue. Instead of aiming to clarify what the issue is based on gathering tons of data, the employer representative now recommends his members to just offer their employees with what the employees themselves can track their well-being without further ado, and one with which they can provide anonymous feedback.

Pseudonymisation involves replacing the easily identifiable information with pseudonyms (e.g., numbers), but the data can still be re-linked to individuals if necessary, meaning it remains personal data. But if it still had, you know, individualised data - just a number without being directly linked to personal data - that is pseudonymised data, but it is still considered personal data according to GDPR.

Data encryption is important, but challenges exist when encrypted data needs to be linked back to an individual, which requires careful management to balance data privacy and utility. Overall, while pseudonymisation allows for continued analysis of personal data, anonymisation ensures that data cannot be traced back to individuals,

offering more freedom for broader use. However, the re-identification risk with pseudonymised data requires robust safeguards to maintain privacy.

No software company fully encrypts data, and that's simply not feasible. The reason for this is that once data is encrypted, you can't perform operations on it anymore - you can't really do much with it. So, in reality, you can't do much with personal data either, except for linking it. If the data is public or anonymous, you can link it to other data sources.

Employees are often also afraid of what the employer will see from that. And yes, also the link to their personal identity, because it's naturally to plan and redistribute work more efficiently. – OS (ALAW)

A last aspect when it comes to anonymity or pseudonymity is that operators themselves should be able, or enabled to decide what can be done with their data. Do they want to share their data in pure anonymity or do they allow data to be brought back to them, and to have analyses made on their data. That is up to them, according to this practitioner.

Another thing we've clearly heard is that for mental well-being, the role of anonymity plays a much bigger role, as well as just the personal aspect. Because it's like a personal diary. Multiple people could be using it, and they can decide what's private or what their settings are for sharing privately, anonymously, or publicly. What are my settings for that, and also giving the freedom to change those settings per report. – OS (ALAW)

In mental health or employee well-being studies, data might be anonymised or aggregated to prevent identification, but it may still be valuable for general insights or trends, such as average stress levels or satisfaction. When it comes to inference, one should be aware to not draw wrong conclusions.

2.5.2 General Data Protection Regulation

The most referred to piece of legislation was without a doubt General Data Protection Regulation or **GDPR**, a European Union regulation on information privacy in the European Union (EU) and the European Economic Area (EEA). The GDPR is an important component of EU privacy law and human rights law, in particular Article 8(1) of the Charter of Fundamental Rights of the European Union. It also governs the transfer of personal data outside the EU and EEA. The GDPR's goals are to enhance individuals' control and rights over their personal information and to simplify the regulations for international business. It supersedes the Data Protection Directive 95/46/EC and, among other things, simplifies the terminology.

The employee representative acknowledges that GDPR is a piece of legislation often referred to when sectoral, national or European legislation is unclear.

Which I have to admit is CAOs, and we still always look at the GDPR first, because almost all innovations that can have an impact on a worker or employee usually do so based on data about those employees. The very first, most important thing. Of course,

or well, they are at work again, I know a bit less about that. That's more for the prevention advisors, which we are less familiar with. But it's a very tangled web of legislation. – PVDB (ACV)

GDPR is often portrayed as a ethically good thing to prevent data misuse. However, as employee representative and lawyer ACV points out, it also brings along some **disadvantages**. In the first place it **individualises** worker rights. The legal perspective in labour is a much more complicated thing, in here there are collective interests that need to be considered. The sum of all individuals consenting with these new initiatives, or on providing their data, does not add up to the collective agreeing upon this. The collective of an organisation has another scope and topicality, and another finality.

Another thing is that GDPR leads to underutilisation of the data, which is in some cases counter-productive. There is sometimes an **underutilisation** of data, particularly within the European framework where we deal with high-tech industries and a knowledge-based economy. We should sometimes encourage the use of data, but for now, this aspect is still underexplored. This can lead to discussions with data protection authorities later on.

A last thing is that employer sometimes **hide behind GDPR** so as not having to share certain data the employee representative feel they have access to. This is an important point, as addressed above in the section of social dialogue, social partners especially employee representatives now and then have the impression that the social dialogue is not open and transparent. Sometimes employers hide behind privacy regulations to avoid sharing necessary information. There's also a need to ensure clarity about data usage and whether employees can later access the collected information. It's crucial for stakeholders, like employee representatives, to understand their rights regarding data access and the process of data collection in the workplace. And now, it has also caused us to sometimes look at things from a different perspective. For example, our representatives, the employee representatives, also need to know certain things about employment within a company. However, they are sometimes confronted with employers who hide behind privacy to avoid sharing certain information. Additionally, it means that we are dealing with many issues. However, this point was rejected by a researcher, lawyer DG:

Fencing with GDPR is an easy argument. Every data subject has the right to data access, but then you see they don't know, they don't know how far reaching it is. It remains unclear in GDPR whether a union can request data from a member. But in that case, I'd say to the unions 'well, try it then, try to request data from a member', and if you don't 'then go to the Court of Justice', or mobilise your employees or partners to request data. I guess they won't do it out of fear of management, or because they lack the digital literacy and awareness. Both employees as well as managers as well as unions do have mechanisms and levers … They should just use them. – DG (UGENT)

The employer representative put it this way:

> **GDPR is of course, a multi-headed dragon. It also applies to you as a trade union, as an employee organisation. We, as an employer organisation, and they, as employees, are also subject to it. So they don't necessarily have the right to data that the employer collects in the workplace. The employment relationship is one of the exceptions in the GDPR, and the information needed within the context of the employment relationship is exempt from GDPR, because otherwise, the employer couldn't pay wages, and so on. But that doesn't mean that other parties suddenly have the right to access that information. So, those same rules apply equally to trade unions.**

Lastly, a practitioner argued that it's not the case that employer are hiding themselves behind the data, the point is that they don't have the data themselves.

> **The first word that comes to mind for me, because I know that, is that the real problem is often that they don't have the data. That's the first reason why I come up with an excuse. They just don't have the data. And then, they might, according to the law, hide behind another law to avoid doing the work and thus not share it, because they're not doing the work, so that's already the first issue. It that it's not always about not wanting to share, but it's just that they don't have it and they don't do it. And they also don't know how to get it. And it's extra work, and the reality is also difficult. Companies, for example, with 1,000 employees, may only have two or three prevention advisors, two or three prevention advisors who need to collect data without having digital systems today, because even digital systems are still new. So, they often don't have the data. That's the reality. That's the first thing, and I know that because I just had a conversation for my company. I said, 'What do you already have? – KDM (VBO)**

2.5.3 Data ownership, control and commodification

When it comes to ownership, control and commodification, it stands out that the employee has to be owner of the data, meaning that he has access to the data whenever he wants, he can decide to provide the data, and at the same time redraw from providing it, or demanding to have his data removed. Companies often need to clarify to employees who has access to their data and for what purposes, ensuring transparency about how long data will be retained.

Consent must be explicitly given, and workers need to be well-informed to reduce the risk of complaints. There are concerns regarding the collection of sensitive personal and health-related data, particularly regarding how this data is stored, shared, and used by employers. There is scepticism about who will have access to data, especially when employees do not fully trust their employer or the algorithms. Employers need to properly inform employees about what happens to their data and ensure they understand their rights under GDPR, including how to exercise those rights.

It should be discussed and there should be **transparency** how the data is stored and how it is processed, and how the outcomes are produced. We preferably indicate where the data is hosted

and by whom. Being transparent about this can help build trust. If you proactively present security measures yourself - such as through a data processing agreement or your own contract - it reinforces credibility and confidence. More so, workers can withdraw consent at any time, which presents challenges, as some may feel uncomfortable about how their data is being used.

And also, yes, that data is local, right, on a watch and then in a local database, or will other things be linked to it? Is the person known in this data? Not known? How long does it stay? That's a piece of GDPR legislation, and how long does that data stay? Is it 30 years? How anonymous is it, how identifiable is it? These are things that you should consider in advance. So yes, here as well, people can indeed say, 'Yes, we want to participate,' but if they withdraw their consent and say, 'I don't want to anymore today,' it must stop, so that's a downside of that. I might say, yes, other processing methods could be considered, but they would be more difficult to implement without consent, and the sensitivity to breaches will be higher. It is important to ensure that you fulfil your duty to inform. That's a large part of it. So, if you ask for consent, they give their consent, and you've sufficiently informed them about what happens with their data.

The chance is small that they can successfully file a complaint, and what they can still do is indeed exercise their rights to information. These rights include requesting information or asking for data to be deleted. – OS (ALAW)

But it's mostly about who can access which data, and why are they allowed to do so? Right? So, man or woman. They all agreed, yes, I remain the owner of that data, and you'll probably make an agreement on that. Certainly, wow. Should I just go ahead with it? Yes, or at some point, it needs to be very clear: Yes, no, which data will be kept exactly? Okay, you're going to use it only for your research, but who, for what purpose, can access which data, and how long will it be retained? Just those kinds of matters. – PVDB (ACV)

In case the data is treated or analysed by third parties, this should be clearly stated. Because overall, the employer acknowledges to have no access to the data at all. It can still happen that external prevention services, for example, connected to a company, will conduct such investigations. But even in these situations, right, the data should never be made available to the employer.

It can still happen that external prevention services, for example, connected to a company, will conduct such investigations. But even in these situations, right, the data should never be made available to the employer. It's meant to protect the individual, right? – DVC (ABVV)

The discussion touched on the practical challenges of managing employee data, including the lack of tools in some organisations and the complexity of managing data privacy effectively. The employer at that moment should ensure that no expectations are created, such as the possibility that might later request the data, as is the case with an external service where you can request certain collective data. For example, it should be clear to every stakeholder to handle it in this way.

That seems important to me, right? If I worked in that company and received all of this as an explanation, then. The employer representative mentioned that due to the restrictions imposed by anonymisation, there not this much that can be done with the data collected. This person therefore argues it is better not to expect to have insights from these data.

I can explain it a hundred times, and they will still always want to collect the data first, while I say, 'Yes, others have already gone ahead of you, and you are allowed to do that, but you will realise that you won't get much from it.' – KDM (VBO)

2.5.4 Legislation: need for dynamism

The GDPR has led many people to focus on obtaining consent, but this is only part of the broader regulatory picture, which includes national labour laws and welfare legislation. These regulations remain important and intact. However, **the dynamic nature of the law** should be acknowledged. Currently, many regulations are static and not adapted to modern technological needs, leading to challenges in staying current. There's also resistance from employer organisations to update laws, especially in light of the GDPR.

But yes, I think the GDPR has simply made many people overly focused on asking for consent, as if once you ask for permission, everything is allowed. However, as you mentioned, this applies only at the company level. There are also regulations from the National Labour Council, as well as other legislation on well-being at work and similar frameworks. Of course, those remain in effect as well. – PVDB (ACV)

But yes, there is a need for dynamism in this, because the legislator must be dynamic. However, today, it is far from dynamic - everything remains very static. Right now, the approach is often: 'We are compliant on paper, so everything must be fine.' But when it comes to creating real dynamism, I see a lot of opportunities. – LT (ACV)

Despite the need for more and dynamic legislation, it was noted a few times that the employer now and then are **reluctant to update legislation**, e.g. when it comes to CAO 39 as well as when it comes to the example given below:

The files and discussions on this topic should ideally be addressed within the National Labour Council. For example, the collective agreement on camera surveillance - we are trying to update it, along with several other regulations. It has been suggested that these should be modernised in light of the GDPR. However, we notice significant reluctance from employer organisations to take any action on this matter. – PVDB (ACV)

2.6 Methodological challenges

2.6.1 Technological feasibility and acceptance

In summary, while sensor-based technologies hold potential for improving workplace health and well-being, there are significant challenges regarding their accuracy, accessibility, acceptance, and the ethical use of data. There's concern about the accuracy of sensors. Employers may overly rely on technology, such as sensors that could be malfunctioning or using the wrong metrics, leading to incorrect conclusions about employee health and well-being.

OK, so how can we think that just by the adoption of tools this indicators will improve, why don't do we peak, do we put or employers or companies put all their hopes on a sensor that might be wrong and might be working wrong, might be using the wrong metrics or might be having a default in order to think or that health and well-being will improve. – LT (XSENSE)

Some technologies, especially new ones, are dependent on personal devices, which may not be accessible to everyone in a workforce. This creates barriers to widespread adoption and consistent use. Other technologies, like machine vision or wearables, may not work equally well for all body types or individuals with different physical conditions. There's also an issue with the effectiveness of some sensors, which can be influenced by skin tone or body type, leading to inequitable results.

Maybe having a fairly normal body type, right? I think that. And after 12 in those machine vision models, they focus on people who have a stocky build, or maybe are in a wheelchair, or have an unusual body shape. 'The technology worked better for people with lighter skin tones, as it required more charging for people with darker skin, which caused less accurate results. This led to a decrease in participation, as some individuals, such as those with larger body types, had difficulty using the device effectively. The issue is noted as being more about the limitations of the technology rather than any form of racism. – LT (XSENSE)

Some solutions may focus on surface-level symptoms rather than addressing the underlying causes of health or productivity issues. Effective solutions should focus on understanding and addressing the root causes rather than simply applying short-term fixes. There are concerns about how employees will accept sensor-based technologies and how the data will be used. There's also the risk of over-relying on technology for decisions that should consider human nuances and context.

2.6.2 Subjectivity

It's difficult to maintain neutrality while also observing problems, and that sometimes employers and researchers must describe the production process as part of the **employee journey.** The data actually, both the physiological and survey data may require contextualisation and interpretation. It is ethically incorrect to argue that objectively quantifiable data have more explanatory power than

qualitative interpretative data. Not recognising the employee journey may cause us to run into flawed interpretations.

An ETUI researcher highlights the importance of analysing both psychosocial and physical harm in the context of well-being and do so both on the short run as well as in the long run, e.g. outcomes such as stress and **physical discomfort may turn up in the short run**, and have physical and mental consequences in the long run. She suggests that the physical dimension should also be considered in analyses of burnout and absenteeism. The researcher stresses that jointly researching variables at the job and task level cross-sectionally, we should be aware that the outcomes in terms of well-being sometimes not readily measurable. An example is that physical discomfort sometimes takes months and years before it shows up. Key message here is that the outcomes in well-being that matter, will **not always be readily measurable**. some employees do not see it as an issue in their day-to-day work. However, he acknowledges long-term concerns like musculoskeletal disorders and the difficulty of balancing neutral observation with potentially imposing concepts or assessments on employees. This reflects the tension between being neutral and addressing real issues.

Because, let's be honest with each other, this data is interesting for you. In the long term, maybe in 10 years, it will bring about a change, but it's not going to change someone's personal situation next year. Employees sometimes have these expectations when such initiatives are being implemented. That's what I'm trying to highlight. So, maybe we should think about a sweetener as an external motivator. – JVD (ACV)

2.6.3 Bias due to flawed interpretability

This issue has been addressed in the section on data interpretability. It relates to the ability of operators to interpret themselves these data, and the availability of a trust person to help them do so in case they are not. From a methodological point of view, this may induce bias, since proper interpretation of data shown is quintessential to guarantee the user (operator) takes proper actions.

Do you always provide those who receive the data, for example, with a follow-up conversation to clarify it? Because I can imagine that if something comes up from it, people might need clarification or further explanation at that moment. I'll tell you, if I see a report and I am the employee being monitored, and there are some parameters that are not okay, then I might need someone to clarify it for me. Is there an option like that built in? And if people have questions, do you provide that information or share it with them, or is that not the intention? – LT (ACV)

2.6.4 Bias due to flawed interference

There is a recognition that when dealing with individual data, particularly subjective well-being data, the accuracy of conclusions can be **influenced if not all data points are available**.

It's not just well-being data. I mean, subjective well-being data, but at times it also involves personal data. So, as soon as you have only half of the data from one individual or no data at all, that also affects the conclusions I can draw. Ideally, we would have everyone on board, but yes, we really need to think of an alternative path for what happens if we don't have data from everyone in a department or so on, because that's the situation, let's say. – PVDB (ACV)

This poses challenges when not everyone in a department provides data. There's also concern about how **different moods or responses** at various times can affect results. (This, however, we of course try to filter out by means of the micro surveys).

Knowing that if you ask the same people again in a short time, the results can be completely different because the mood of the day affects all the answers. Of course, this isn't the case within a sound meter, but yes, that culture of 'measure to know' is there, and even all the newly graduated safety advisors. They can't be convinced to say, 'dare to measure but don't measure,' and instead use a tool we know has positive effects - they will never do that. Hence, there are always organisations that say; - RH (VUB)

Furthermore, while people may initially view their well-being data as private, there's a belief that once individuals realise there are issues with their data, they will eventually share it. The question then is if the company has someone (trust person) in house who is readily available for this person, and for instance, if the operator aims to discuss the data with other people, for instance, husband, friends, psychologist, whether she will be able to do so?

Most people today tend to say, 'It's completely private.' But I'm convinced that when people have actually collected the data, at some point they will say, 'Oh, I actually have a problem in this area.' Then they will feel the need to share it with someone. Yes, we believe that. But the initial reactions are, 'Well, this is really private, how I feel mentally, or physically.' – LT (XSENSE)

However, some worry about the risks of **drawing conclusions from correlations alone**, what we see happening today increasingly (with big data analytics) without establishing causation, which could lead to misuse of personal data with serious consequences.

The question is also, what kind of mistakes are starting to be made again, so much data that correlation is enough, we no longer need causation, leading to dangerous conclusions. Then you can quickly see abuse of personal data, with far-reaching consequences, the relationship between data and the conclusions drawn from it, and what those conclusions imply for the individual and their loved ones. – DG (UGENT)

2.6.5 Bias due to flawed validity

When it comes to validity bias six interviewees touched upon the issue, measurement results, particularly heart rate variability (HRV) data, which by **itself is insufficient for conclusions**. It highlights the need for combining different research methods to ensure accurate results.

Or was it that it was very, very important to validate the heart rate variability results, which by definition are insufficient to validate with this kind of diary research. And that's a combination, this combination research that's the most. – MC (EU OSHA)

Some experts argue that understanding stress levels or ergonomics doesn't always require detailed measurements, and that specialists who work directly with issues like repetitive movements can offer valuable insights without relying solely on data. The following quote illustrates that subjective indications operator-based may sometimes be more valuable than intensive measurement. Between the lines I read that we do not want to surpass or bypass those that are truly active in the field. In other words, **should we really aim to objectify well-being** risks or the well-being status and impose that status on someone who can thing for him or herself? This raises the question about whether objective and subjective data are juxtaposed, or one type of data can or should be given more attention than the other since it may 'rule out' the other type of data.

Problems with ergonomics, lower back issues, and other real problems caused by constant repetitive movements. For this, we don't necessarily need to measure every detail, but we should listen to the specialists who work day in and day out and know what the biggest challenges are. On the other hand, you don't really need sensors and abstract measurements for everything. In my opinion, the real specialists are the ones who are on the shop floor, the ones who work with it day in and day out. – JVB (ACV)

Additionally, the integration of physiological data with subjective experiences is emphasised, as it is important to **balance objectivity with personal perception** to improve the validity of the measurements. There's also discussion about whether subjective data can be reliably quantified, raising questions about what data is necessary and what is ideal for measuring well-being at work.

To what extent can you substantiate that the data you collect is actually a good indicator of well-being at work? HRV is an indicator of many processes. The question is, what is the trade-off for the employees who are going to release the data? Can we learn something from the data? My question would be, why do you use physiological data? Is subjective experience more valuable? I try to objectify subjective experience, but psychologists seem to struggle with this. What about reliability? Can you, the lawyer in me wonders, why would you measure all these physiological data - why do you do that? I see that measuring is knowing, but have you considered what is necessary and what is desirable, and have you distinguished the latter two? – RH (VUB)

There is an ongoing debate about whether physiological data are to be prioritised over subjective experiences. Psychological experts face difficulties in objectifying subjective experiences, raising concerns about data validity. External factors, such as flawed smartwatch readings, can introduce **noise into data**, making it unreliable for serious decision making.

2.6.6 Bias due to flawed reliability

While digital and physiological stress measurements provide valuable insights, their reliability remains uncertain. A cautious approach—balancing subjective experiences, expert judgment, and validated data—is essential to ensure accurate and ethical workplace assessments.

Stress levels can be influenced by both work and personal life, making it difficult to attribute causes solely to workplace conditions. Employees experiencing stress at home might still perform well at work but could be unfairly evaluated based on physiological indicators like heart rate. Over-reliance on individual stress measurements can lead to misinterpretations in performance assessments. This may lead to attribution error.

Someone experiencing a lot of stress may be affected partly by work but also partly by their personal life. If stress levels are measured - let's say someone is told, 'We notice you have high stress today,' - then the question arises: How reliable is this measurement? For instance, a person may naturally have a higher heart rate due to physical factors. So, how directly can stress be attributed to work alone? From a legal perspective, it's important to ask: To what extent is there a clear one-to-one relationship? And are other parameters taken into account when making conclusions? Understanding stress levels is one thing, but if there are dozens of other correlations, then the cause may be something entirely different. – DVC (FOD WASO)

Occupational health and safety professionals face difficulties in interpreting new data due to its **unproven reliability.** There is a lack of validation for workplace health sensors and monitoring apps, leading to concerns about their effectiveness in decision making. Employers and professionals struggle to determine whether the available data is trustworthy enough to guide workplace policies.

They don't know. There's no information on on. Is this app good enough? Is this sensor good enough? Or. What is good enough it can I? Can I make decisions ongoing? Can I make decisions on the health, or the life and death of my employees based on a sensor which is nobody knows how reliable actually is? – AS (EU OSHA)

Relying solely on sensors and digital metrics may not be sufficient for understanding workplace conditions. Experts working directly on-site often have more accurate insights than abstract digital readings. Digital stress measurements provide only momentary snapshots, lacking the depth of long-term observation methods like motion capture.

2.6.7 Bias due to self-selection (participation bias)

Participation bias or non-response bias is a phenomenon in which the results of studies, polls, etc. become non-representative because the participants disproportionately possess certain traits which affect the outcome, in the case of this project operator well-being. Ensuring diverse and representative employee participation is crucial for reliable workplace studies.

Companies use broad communication strategies to recruit participants, but selection can be biased **if only certain employees volunteer**. Based on one of the interviewee's experiences, this voluntary participation may skew the outcomes. In the example that follows, workers experiencing the heaviest workload may use participation as a way to voice complaints about job strain:

> **They secretly wanted to file a complaint about the heaviness of their work because they were the ones who indeed had the hardest and most physically demanding jobs. In such cases, it is best to propose selecting employees from different groups. By picking 3 or 4 from each group, we have a much higher chance of obtaining a representative average. A purely random sample is, I think, the best approach, so ideally, even selecting entire teams. – JVB (ACV)**

When it comes to companies, there is also a remarkable to mention. There may not only be bias on the employees that would be happy to participate, but more so, also in the companies that present themselves (in our case to the user group).

> **Participation of workers in decisions related which have an impact implications for us. So in a way, there is also a sort of bias in our research, meaning that we find always like companies that are happy to be involved and be part of a case. The only because they're for performing goods we I think that we never have, you know, access to companies that are not performing good. But for us this is not really a problem one we have also that, but we the thing is that it's not really a problem, because that means that these principles of worker participation, workers, information, developmental trust, et cetera, are the good thing to do. – JVB (ACV)**

This may limit insights into less successful companies, though participation still fosters transparency and worker involvement. Stress can act as a barrier to participation, as highly stressed employees may not have the time or energy to engage in studies. This can lead to skewed data, where results mainly reflect the experiences of less-stressed individuals.

2.6.8 Bias due to data manipulation

This section discusses concerns about the manipulation and reliability of workplace monitoring data. Employees may find ways to influence their physiological measurements, such as moving excessively to create misleading activity data or using external tools (e.g., attaching Fitbits to metronomes) to deceive employers about their physical activity.

Yes, I realise now that not only the employer but also the employee could misuse this data - for example, by moving intensively at their workstation to avoid their tasks. These are all things we take into account.

Manipulation of data indeed happens when people know which specific metrics are being measured and how they can benefit from them. For instance, if your heart rate needs to be extra high or extra low, you might try to influence the measurements accordingly.

Some people have even studied ways to cheat devices like Fitbits, which employers use as a form of self-surveillance. There are at least 20 different tricks, such as attaching the device to a metronome or a bicycle wheel, to falsely record steps and make it seem like they are staying active at work. – RH (VUB)

There is also debate about whether long-term physiological data collection can be reliably manipulated. Some argue that sustained data manipulation is unlikely, especially if sensors are integrated into work clothing over extended periods. Employers tend to trust sensor-based monitoring more, believing it provides more objective data. However, these concerns highlight the broader issue of data integrity and ethical implications in workplace surveillance.

Because I would expect that in the long run, only those who can truly sustain it will keep up. So, over a long enough period, it's true that just a week or so is not enough. But if you really look at it - Michiel, this is what we're focusing on - we believe that the future lies in integrating this technology into work clothing. We understand the technological challenges, and we will work over the next few years to overcome them. We believe that if this technology becomes part of clothing, then over the course of a year, you won't just be relying on temporary measurements - people will be able to sustain and track data for a much longer period. – JVB (ACV)

More so, workers may both manipulate survey responses as well as physiological data to benefit themselves, particularly in environments where job security or pay is uncertain. Workers in organisations with better conditions might present more positive feedback, while those in less favourable environments might be more negative, hoping for better benefits. This highlights the subjectivity and reliability issues with surveys and data collection.

There's mention of using technology to track workers' physical activity or stress levels. However, notes that it's difficult to get reliable data over time, as workers may manipulate their behaviour (e.g., by artificially increasing their physical activity) to influence measurements. The data gathered from such methods, especially when used to assess calorie consumption or stress, can only be collected over short periods without causing discomfort or stress to workers.

And when there are indeed layoffs, there is the fear that those who indicate a poor work environment will be seen as victims. The labour relations are not good, people vote negatively, and so on. Or they might say they sleep well at home, but they actually

consider themselves victims. Then they try to present things more positively than the reality. Those in companies where things are going well will say things aren't bad because they say, 'we're making a profit.'

Here, job security is present. I'm not in danger of losing my job, we can always improve, and by presenting things more negatively, they hope to get more benefits, higher wages, more days off, and so on. But they think it's a risk they're willing to take. So, with these surveys, the reliability is very socially or situationally dependent. Is this something that organisations are aware of? – PVDB (ACV)

2.6.9 Bias due to instrumentation

Instrument bias emphasises that the **use of technology to monitor** workers' performance can contribute to increased stress and mental health issues, with some workers reporting depression and other problems when constantly being monitored. This raises concerns about the balance between data collection and worker well-being.

They report as well increased stress. They report more like, I don't know, indicators as depression or other, you know, mental health problems. So there is some quantitative evidence as well. It's clear that when workers have this perception. […] Yeah, I can't use anything, and to do that, they indeed looked at how many calories someone burns based on their heart rate, breathing rhythm, the volume of breath, not just the rhythm, but also the exhalation. But you can only do this for a very limited period of time. Only a few people can do this because otherwise, people start sweating from the stress of the 10th of those shifts. – MC (EU OSHA)

2.6.10 Resistance to participate

While workplace data collection can provide valuable insights, ensuring **voluntary participation** and addressing employee concerns about anonymity and coercion are crucial for maintaining trust and cooperation. Employee surveys, such as satisfaction questionnaires, are typically voluntary, though some demographic categorisation (e.g., worker type, role, or shift schedule) may still be identifiable. This is questionable. Operator may not want to be incorporated in the research, still though, **aggregate conclusions** may be drawn about them. The question that also rises is 'how voluntary is voluntary?' What about peer pressure, team pressure. If not filling out questionnaires, taking part in the research may raise suspicion among colleagues.

Employees may resist new data collection methods, especially when they feel coerced into participation. Resistance can create tension in the workplace, highlighting the importance of giving employees the choice to opt in or out of data collection initiatives.

I think I would be open to that, but have you already asked that question to implement it in a company, or how does that look? Because, yeah, I wonder if everyone is open to that. And then resentment arises. People tend to resist quickly, but well, those are personal experiences that you've probably already taken into account. No, I think it can

definitely work, but do people have the chance to refuse to cooperate, or do they have to cooperate? – LT (ACV)

2.6.11 Measurement beyond intent

This section highlights concerns about trust and data misuse in workplace monitoring. Employees are often suspicious about how their data will be used, even when collected by occupational health professionals. There is fear that data could be misinterpreted or used against them, leading to a lack of trust in employers.

Additionally, research shows that data collection sometimes exceeds what is strictly necessary, capturing personal information beyond legal requirements. Automated worker management systems have been linked to increased stress, depression, and other mental health issues, raising ethical concerns about the impact of workplace monitoring technologies.

But we are aware as well of the fact and this has been reported in many interviews with stakeholders, that sometimes these data collections goes beyond what is strictly necessary or strictly the you know, Legal event. And they are also a lot of personal information are collected, etcetera, etcetera. Now the problem that we found is that in the literature also in Europe it is different. There is a bit of a difference in that in the literature it's mentioned that for example, in the automated systems for worker management this this umm data are used for example. Technologies were used to perform, you know, to monitor their performance, etcetera. They report as well increased stress. They report more like, I don't know, indicators as depression or other, you know, mental health problems. So there is some quantitative evidence as well. – RH (VUB)

2.7 Ethics in relation to various contextual characteristics

2.7.1 Ethics of defining well-being at work

The definition of well-being has been touched upon in five interviews. Firstly, it was noticed that the well-being of employees in general (operators in particular) may be subject to being increasingly operationalised through **data-driven approaches**. Five interviewees argued that there are now tons of data, and were pretty sceptical about whether these data could truly identify how the state of well-being among employees would be. To be specific, these interviewees argued that simply accumulating data (being either physiological or survey data) would not add up to increase our understanding of well-being at work. More so, one observation was made that we nowadays have the tendency to just being happy with (big) data correlations instead of seeking ambitiously for parsimonious causation.

Secondly, the conversation touched on the importance of **properly understanding the concept of operators' well-being**, and not only from a researchers point of view, but also by hearing the operators themselves. Key will be to truly understand and define operator well-being to ask the people in the field how *they* see it, what the challenges are that *they* face, and how to address

these issues effectively. Participants highlight the need for businesses to align their methods for assessing well-being with the real challenges employees face. This is nicely exemplified with a quote from one of the researchers interviewed:

In Flanders, there is also a broader focus on making work *workable* which involves constantly adapting the workplace to evolving job requirements. This **adaptability, the flexibility, the ability to be flexibly deployable** is considered key to creating a healthier work environment on the long run, where employees can remain engaged and productive. One of the interviewees argued that this dimension may be a bit missing in our framework.

Lastly, one of the interviewees shifted the conversation on well-being at work, by raising it to another level, emphasising that well-being in the workplace is so multi-layered and multi-dimensional that we may want to **look beyond business-level solutions**, by also incorporating care systems into this debate (and into the technological methodology). More so, we should consider at a more societal level, not only the needs and capabilities of employee X in company Y. We should strive to look beyond, by matching employees' skills and interests to suitable jobs becomes in the entire society (i.e. the labour market). The role of policymakers is also mentioned, suggesting that they should offer more flexibility to companies, allowing them to innovate while maintaining a focus on well-being.

2.7.2 Organisational and contextual differences in privacy and ethics

Throughout the interviews, it was notices that organisational maturity and organisational trust seemed to few interviewees a quintessential precondition to make sure that the introduction of technological methodology would succeed. Employees need to trust the technology and the employer for well-being data to be effective. This **trust** can be built by transparent communication and ensuring employees know that feedback from data is intended to improve their work, not to monitor them.

For effective integration of well-being programs or digital technologies (like wearables), the employer must demonstrate commitment and create a participatory environment. Employees must feel safe and valued, without the fear of surveillance or loss of control. Some companies may struggle with these concepts, especially if they lack organisational maturity or have a typically, classical **hierarchical structure** where employees may resist such changes. Without management commitment and trust in house, any initiative, well-being or other, may face limited acceptance. In environments where trust is low, data-driven initiatives may be met with scepticism or rejection, and company culture must prioritise clear communication, safety, and support to foster employee well-being.

This also closely relates to the role of and the connection with **the unions in the organisation**. This is an extra layer of trust that needs to be guaranteed. Events of the past, and how thing were have been tackled in the past do have some path-dependency. So in cases were trust got lost due to certain events, rebuilding trust is quintessential to make sure these initiatives are experimented with, and will eventually succeed.

These aspects were also underlined, and positioned in the light of employer organisations. The following quote illustrates that not only the connection and the expectations with the employee representatives, but also with the **employer representatives** should be aligned.

2.7.3 Cultural differences on the ethics and privacy requirements

According to X interviewees, there is a cultural shift happening around the sharing of data. In what follows, we discuss the observations that relate to various context, and detail some aspects that relate to particular cross-country differences.

A first generic observation is that people today are becoming more accustomed to **freely so to say giving away their data**, often without fully understanding the consequences. The sharing of personal data has become so normalised that even educated individuals and professionals don't fully grasp the risks involved.

There is, as indicated in an interview (DG, UGENT) an importance to **create a sense of urgency and a sense of (data) awareness** about the potential nefarious consequences, as it's difficult to reverse the data-sharing once it's done, and there is a lack of awareness about what can happen with the data afterward. Nowadays, this interviewee argues, there is definitely a lack of awareness regarding the unintended adversary or perverse consequences, such as how the data could potentially be used against them. In some cultures, data is shared openly, and it becomes challenging to retract once given. This sentiment was echoed in a conversation about the difficulty of reversing the decision once someone shares their data.

A third observation with regards to the cultural differences refers to cross-country differences on the **perception of privacy and ethics**. For instance, in countries like the Netherlands, there is much more openness when it comes to data sharing, and there is much more awareness and a spirit driving innovation regarding workplace well-being and data collection. As such, one interviewee argues that people in the Netherlands are more engaged in discussing these topics and actively working together to improve systems, whereas in Belgium, the approach tends to be more institutionalised, with less focus on innovation and more emphasis on following regulations.

> **You also notice a difference between Flemish, Walloons, and Dutch people. There's much more openness in the Netherlands, so you can see that culturally, it's tied to a lot. It's not that everyone thinks the same way about privacy and the ethics surrounding it. Some people really want it to be known that they've been seen or considered by the company. Others prefer to keep it personal and maybe share something at a certain moment, or maybe not. – LT (XSENSE)**

A fourth observation is that this so-called cross country cultural divide is also visible in the varying **institutionalised contexts** countries when it comes in particular to safety and prevention, as well as the handling of data. While in the Netherlands, there is a proactive approach with competitive efforts to innovate and improve (intensified by the free market approach towards dealing with organisational health and safety, ergonomics and the like, in Belgium, the focus is more on maintaining compliance and following established institutions (being for instance the social partners), which function as a solid basis to reach out to, but, to one of the interviewees, may also cause the topic of safety and prevention running into a standstill, and hinder progress.

2.7.4 Cross-country differences in ethics and privacy related to well-being at work

In this section, just one of the interviewees discusses the differences between countries in terms of workplace well-being, particularly in Europe. He highlights that some countries lag behind in embracing the potential of digital tools, especially in the context of health, safety, and employee well-being. The person points out that while some countries, particularly the Baltic states, have a good reputation for digitalisation, they still lag behind in terms of safety and health measures. These countries have a culture that is more open to adopting digital tools, making it easier for them to move forward, even though their well-being systems are less developed.

Countries like Italy, Spain, and Eastern European nations struggle more because they have not fully embraced digitalisation and continue to rely on traditional industrial structures and outdated labour models. These countries face the biggest challenges in integrating digital tools with workplace well-being systems.

He also touches on the Scandinavian model, where there is a strong desire for countries to manage social dialogue and welfare internally without interference from the broader European Union. Scandinavian countries prefer to maintain control over their policies and practices regarding social and labour issues.

Despite these apparent differences across countries (and essentially welfare regimes), he notes that in every country, there are examples of pioneers or opportunists who have created business models around this issue and are leading the way. Finally, he mentions a global organisation with an impressive database that manages the health and well-being of its workers, particularly in the medical field. He highlights their 'duty of care,' ensuring that employees have access to healthcare and other resources. The organisation's headquarters in London is described as having one of the most impressive systems for managing employee health data.

In summary, the interview discusses the variation in how European countries approach digitalisation in the workplace and well-being, with particular emphasis on challenges in Southern and Eastern Europe, and the examples of progress in places like Scandinavia and the Baltic States. The importance of 'duty of care' and access to healthcare within organisations is also highlighted.

2.7.5 Sectoral differences on the ethics and privacy requirements

Five interviewees outline sectoral variation with regards to collecting operator well-being data. Firstly, when it comes to surveillance and worker well-being, interviewees argue that workers in the port are and have always been heavily surveilled. In such sectors it may be easy to build analysis on the operators well-being upon existing monitoring realities. The same goes for the petrochemical industry, where steps in the production processes regularly need to be authorised, where boxes need to be ticked off, etc. Here, there is already an awareness about data running in the organisation, and there are already regulations on these data.

Secondly, each sector faces its unique and institutional challenges when it comes to approaching well-being at work, in the interview one of the five mentioned, referred to construction and petrochemicals. In industries like petrochemicals, the focus is often on maintaining the integrity of installations, which sometimes leads to more attention on worker safety and health. Meanwhile,

industries with lower-skilled, manual labour (like construction) are seen as lagging behind in these areas.

Thirdly, when it comes to **social dialogue**, there is quite some sectoral variation in the frequency and topics when it comes to the meeting unions and employer organisations engage in. In some sectors the social dialogue is more structured (e.g., construction) compared to others that only sporadically address operator well-being. More so, the effectiveness of sector-wide initiatives w.r.t operator well-being is also closely tied to cultural readiness of companies, trust within the companies.

Fourthly, in some sectors, **economic realities** are certainly and rapidly pushing for better working conditions, especially as labour shortages force companies to reconsider their practices. While sectors like construction face challenges in improving workplace conditions due to economic downturns, others (like for example the industrial cleaning sector) have been more successful in adopting digital technologies that enhance worker well-being.

Overall, the interviews so far highlight a need for clearer communication, better sector-specific strategies, and a more holistic approach to improving worker well-being, especially in industries with manual labour.

Lastly, however, the research expert from ETUI shows a critical attitude towards the work practices and **working standards, being created by and determined by industry players** rather than workers. She points out that workers in general are not consulted or involved in truly shaping their work practices, nor in shaping their standards. A probable issue with the technological methodology then would be to draw conclusions about our UG cases and aggregate these to the entire sector. Despite the degrees of freedom, the technological methodology

2.8 Relevant parties

This section explores the diverse perspectives and roles of key stakeholder groups involved in the development, implementation, and regulation of employee well-being measurements and technologies. It aims to highlight how various actors, ranging from workers and employers to external consultants, legal advisors, and regulatory bodies, experience and respond to the ethical, practical, and privacy-related challenges associated with these tools. By presenting insights from each group, the section outlines both their responsibilities and the concerns they raise, including issues of transparency, participation, knowledge gaps, and accountability. The analysis also draws on direct reflections from stakeholders to illustrate the complexity of navigating well-being interventions in contemporary work settings.

2.8.1 Workers/employees

- **Concern for well-being**: workers are often concerned about their own well-being, with some fearing that the data being collected might be used to their disadvantage. The notion of ‘data surveillance’ in the workplace raises privacy issues for employees.

- **Participation in decision making**: employees need to be involved in the decisions about tools and technology implemented by employers, especially when it comes to monitoring health, productivity, and safety.

- **Lack of knowledge**: workers may not fully understand the implications of the data collected on them, leading to a lack of control over their privacy.

- **Potential resistance**: workers, especially in blue-collar jobs, may resist new technological tools due to a fear of being monitored or penalised based on data (e.g., data-driven performance evaluations).

2.8.2 Employers/companies

- **Providing well-being tools**: companies are introducing tools aimed at increasing employee productivity, but there is concern about how these tools affect employee privacy. Employers are often depicted as trying to balance the use of data with maintaining worker trust.

- **Data collection**: employers are collecting data on workers, but this data can be seen as intrusive. It's noted that employees may not always be comfortable with the amount or type of data being collected.

- **Lack of communication**: companies may not always be transparent with their employees about how data is being used, contributing to distrust. Some employees feel like they don't have enough information about what is happening with their data.

- **Employer responsibility**: there is an emphasis on employers taking responsibility for the ethical use of data, respecting privacy, and ensuring well-being, especially in industries where data collection is integral.

2.8.3 Third parties

- **External preventive services**: these services are seen as beneficial in supporting employee well-being, especially regarding physical health and safety. There is a desire to engage these third parties more in the design of well-being strategies, but coordination can be complex.

- **Consultants**: consultants are often seen as external experts that help companies implement well-being programs, but there's a suggestion that their role might be limited to top-level implementations without fully addressing workers' concerns.

- **Innovators/Innovation managers**: innovators are pushing for the adoption of new technologies to improve worker well-being and productivity. However, the challenge is often in balancing technological advancements with respecting privacy and maintaining ethical standards.

- **External data protection officers (DPOs)**: these professionals are mentioned as crucial for ensuring that data collection practices comply with privacy regulations. However, they might have limited involvement in decisions that directly affect workers.

- **Sectoral partners**: partners that sometimes have their own sector specific initiatives.

2.8.4 Trade unions/workers' councils:

- **Unions as advocates**: trade unions are seen as key advocates for workers, ensuring that employers cannot misuse technology or data to disadvantage employees. They play an important role in negotiating better conditions for workers, including data privacy concerns.
- **Challenges in representation**: there's a sense that unions, especially in larger companies, might struggle to fully understand the technical aspects of new well-being tools. Additionally, some workers feel that unions are not fully aware of or involved in new data practices.
- **Works councils**: these councils play an important role in representing workers' interests in discussions about well-being. However, there are concerns that these councils may not always have the required knowledge or power to influence decision making on digital tools and data collection.

2.8.5 Regulatory bodies

- **Data controller**: this legislative entity determines the purposes and the means of data processing, and is legally responsible for DPL. If multiple actors or organisations are involved, a 'joint controller' refers to the combination of all parties that jointly have to discuss their respective responsibilities for complying with legislation.
- **Data processor:** this legislative entity processes personal data on behalf of the data controller and is usually an external party with specified duties, e.g. offering IT solutions, including cloud storage.
- **Data protection authorities**: these bodies ensure that companies follow data privacy laws (like GDPR) when it comes to the handling of employee data. There is a concern that these authorities may not always be able to adequately regulate the growing use of digital tools in the workplace.
- **Ethical committees**: ethical committees are seen as important to ensuring that the use of technology and data collection for well-being purposes does not cross ethical boundaries, such as violating privacy or exploiting workers.
- **Compliance with laws**: regulatory bodies are seen as necessary to ensure companies comply with both national and international privacy laws, particularly when dealing with sensitive data such as health and performance metrics.
- **Privacy committees**: these internal committees ensure that the company adheres to privacy regulations, especially in terms of data collection and usage. They must be involved in every step of the process to ensure compliance.
- **Legal advisors**: legal professionals are responsible for advising employers on the laws surrounding data privacy, ensuring that well-being data collection complies with relevant privacy regulations.

2.8.6 Health & safety stakeholders

- **Occupational health and safety advisors** (in Dutch: 'Preventieadviseurs'): these experts are seen as important for maintaining workers' health and safety in the workplace. They are involved in providing advice and guidance regarding ergonomics, safety standards, and mental health.
- **Medical/Health services**: occupational health services are crucial in assessing the physical and mental health of employees. They may be involved in wellness programs but also raise concerns about the privacy of health-related data.
- **Health and Safety Committees**: these committees are tasked with overseeing the overall well-being of employees. They often focus on physical health and ergonomics, but there is also a growing recognition of the importance of mental health in the workplace.

2.8.7 Technological/data tools stakeholders

- **Tech developers**: developers are at the forefront of creating tools that monitor employee productivity, health, and safety. The challenge here is ensuring that these tools are effective without infringing on privacy rights.
- **Software/Tool providers**: external companies that provide software solutions for monitoring employees are often seen as essential, but also sometimes as contributors to potential privacy violations. These companies might not fully grasp the ethical implications of their products.
- **Technology innovators**: these individuals or teams are pushing for more advanced tools that can help improve employee well-being but often fail to address concerns about privacy. Their role is to innovate, but ethical concerns around data use must be factored in.

2.8.8 External experts

- **Psychologists**: experts in mental health are consulted for advice on managing the mental well-being of employees. They stress the importance of considering the psychological impact of monitoring and surveillance technologies on workers.
- **Ergonomists**: these specialists focus on improving the physical comfort and safety of workers. There is an emphasis on ergonomics as part of an overall well-being strategy, alongside other physical health measures.
- **External consultants**: external experts and consultants can provide valuable insight into well-being strategies, but there are concerns that they may not fully understand the nuances of privacy and data issues in the workplace.

2.8.9 Cross-border/International Stakeholders

- **European authorities**: these bodies are important for overseeing data protection across Europe, ensuring that companies across different countries comply with European standards, such as GDPR, when dealing with employee data. [outside the scope of this project]

- **Cross-European practices**: collaboration across borders is essential to establish standardised practices in employee well-being and data privacy, with a focus on ethical practices in handling sensitive information. [outside the scope of this project]

3 CONCLUSION

The interviews provided rich and nuanced insights into the ethical, legal, methodological, and contextual challenges of implementing well-being monitoring technologies in the workplace. They revealed concerns not only about the outcomes of such technologies but also about the processes leading to their adoption, highlighting tensions between stakeholders and underscoring the importance of transparency, fairness, and participation. The interviews also drew attention to the diverse roles and responsibilities of various actors involved, from employers and workers to legal advisors, unions, and health professionals.

Together with the findings from the literature review, the interview insights form a comprehensive foundation for developing a set of structured design requirements. These requirements, presented in the final part of the report, aim to ensure that the WellFiciency methodology is implemented in a way that is ethically responsible, context-sensitive, and practically viable.

PART 3
DESIGN REQUIREMENTS

Introduction

The third part of this report is dedicated to the privacy and ethical requirements to be taken into account in the WellFiciency-project. Importantly, we hereby particularly focus on the *specific requirements* that apply to the current project. To this end, we thus depart from generic privacy and ethical recommendations when it comes to developing, implementing and using a technological methodology to support employee well-being, more precisely, operator well-being (OWB). It is, however, equally important to mention that we base ourselves on two different sources of data. Firstly, we base ourselves on the literature on monitoring and self-monitoring technologies and employee well-being. Secondly, we draw from 25 interviews with various sorts of stakeholders (e.g. practitioners, research experts, social partners). These parties firstly gave their general thoughts of this topic, and upon presentation of our project, applied and concretised their recommendations to the scope of our project. This part of the report should in that sense be seen as a summary of literature and expert interviews, applied to the requirements of the WellFiciency-project.

The following three paragraphs briefly summarise the precise aim of this project in terms of the three delineated outcomes that should result from it. We do so, since these three expected outcomes will be the subject of our exercise on privacy and ethical design requirements. After that, we define a structured list of design requirements. The WellFiciency-project is aimed at realising a technological methodology supporting operator well-being by means of three concrete and closely related initiatives. These initiatives are the three project outcomes or results that can be summarised as: (1) a digital twin of operator well-being, (2) a person-based well-being dashboard, and (3) a well-being-aware allocation and scheduling optimisation tool that has an online (real-time) application and an offline application, and in each case provides recommendations.

To start with, the **digital twin** is based on the conceptual framework (Bal & Dessers, 2024). Essentially, the digital twin operationalises the central concepts of the latter framework. It does so in particular with three instruments: with a baseline survey, with micro-surveys and with various sensor technologies. Each instrument aims to reflect a physical and/or cognitive composite that may explain operator well-being and thereby contribute jointly to a holistic understanding of operator well-being. The data collected with the various instruments will '*correlate objective (physiological) and subjective well-being metrics, production data, and relevant contextual knowledge'*. After that, inference algorithms will be employed to '*segment and interpret raw well-being data into higher-level well-being insights'*. Importantly, the digital twin of operator-well-being proceeds the person-based dashboards as well as the well-being aware allocation and scheduling recommendations.

Then, the **well-being dashboards** (onwards dashboards) are then a representation of the digital twin. The purpose of this dashboard is to empower operators by allowing them to understand the effect of the individual tasks on their well-being. At the same time, the dashboard will (may) facilitate the communication of and about well-being data with other stakeholders, aiming to render '*more stable and sustainable employee-employer relations*'. The dashboard will be implemented as a web browser application to warrant platform portability. The well-being is customisable and person-based so that each user (operator) may focus on certain particularities of preferences. The dashboard is essentially built out of advanced physical and cognitive data. As an example, the physical data will be based on multimodal physical sensor data (e.g. posture, ground reaction

forces, muscle activity and joint torques when it comes to physical load), but also on micro-survey indications, and will be situated in the baseline survey.

Lastly, the **well-being-aware allocation and scheduling recommendations** (onwards allocation and scheduling tool, abbreviated as allocation tool) are to be based on an automated offline and online scheduling tool. This tool will additionally to traditional scheduling tools (that account for sets of tasks, sets of operators and sets of work stations) also take into account physical and cognitive composites as well as preferences and competences of the operators. In general, suggestions of task allocation and scheduling will be provided based on (1) operator characteristics (e.g., preferred level of task variation, task preferences, competences), (2) task characteristics (e.g., physical demand of task, stressor probabilities), (3) job characteristics (e.g., level of task variation during a shift), and (4) productivity-oriented criteria (e.g., task times, precedence constraints).

Having summarised the aim of this project by specifying the three central project outcomes, this part now brings about the ethical and privacy related design requirements.

In doing so, we will follow the ethical principles of deontology and those of consequentialism. Put simply, deontology contends that the ethical evaluation of an action (e.g. developing a technological methodology to support employee well-being) should be related to the *intention* (and not on the consequences) of this action. In general, an action is not *allowed* if actions are not universalizable. Consequentialism is different. Whether an action is ethically right or wrong depends on the *consequences* of the action, not on the intention and the motivation. The design requirements will be evaluated in terms of intention (i.e. deontology) and outcomes (i.e. consequentialism). Why so? Firstly, we do not only abide by deontological principles without considering the well-being consequences. Secondly, neither do we ignore the deontological principles, even though the consequences for well-being would advance. These universal ethical frameworks will now and then come back to the fore when we bring about the design requirements.

Prior to that, important definitions are set out. ‘Personal data’ are defined as any information related to an identified or identifiable employee. ‘Processing’ is understood in a very broad sense (GDPR, Art. 4, 2) and contends any manual or automated operation on personal data, such as ‘*collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, disclosure, transmission, dissemination, use, alignment, combination, restriction, erasure or destruction*’. In addition, we define three roles that are associated with processing personal data. ‘The data controller’ firstly determines the purposes and the means of data processing, and is legally responsible for DPL. If multiple actors or organisations are involved, a ‘joint controller’ refers to the combination of all parties that jointly have to discuss their respective responsibilities for complying with legislation. ‘The data processor’ secondly processes personal data on behalf of the data controller and is usually an external party with specified duties, e.g. offering IT solutions, including cloud storage. Thirdly, ‘the data protection officer’ (DPO) is a designated (internal or external) personally responsible for the data protection strategy and compliance. He or she monitors data protection activities and acts as a point of contact between the organisation and regulators. In cooperating with any third party, this may change the dynamics of how employers (aim to) share legal responsibilities. Importantly, third parties cannot fully reduce employers’ legal responsibilities of safeguarding employee data (Nunan & Di Domenico, 2017).

The design requirement themselves are categorised thematically. The following paragraphs define *process ethics* regarding the development of the methodology, *outcome ethics* regarding the

expected consequences, *legal frameworks* and *methodological challenges* when it comes to developing and evaluating a such a technological methodology. The aim is to make these design requirements as practical as possible. And, as mentioned, the foundation and rationale behind the requirements can be found in the literature review and the interview results.

1 PROCESS ETHICS

Are we making ethically desirable decisions during the development of our technological methodology? This question relates back to deontology and is associated to the *intention of the action* (and not on the consequences) of this action. In general, an action is not *allowed* if actions are not universalisable. We discuss participation, social dialogue, data literacy and data awareness, and communication

1.1 Participation

Participation in the development is required. The depth, breadth and temporal stretch of participation range from (at least) superficial information and consultation at one moment in time on the one end, to (at most) continuous or repetitive meaningful involvement. {three legal principles}

- The **depth** of worker participation has to be discussed.
    - The operator is involved when it comes to the purpose of the methodology.
    - The operator is involved in conceptualising and constructing well-being. (*digital twin*)
    - The operator is involved in developing mechanisms that lead to well-being. (*digital twin*)
    - The operator is involved in choosing the technologies of use. (*digital twin*)
    - The operator is involved in designing and adapting the *dashboards* and the *allocation tool*.
- The **temporal stretch** of worker participation has to be discussed (regarding *digital twin*, the *dashboards* and the *allocation tool*). The process-oriented approach has been legitimatised in the European Social Partners Framework Agreement on Digitalisation.
    - The operator is involved at the start of the project.
    - The operator is involved over time, i.e. during the process of development.
    - The operator is involved in planning the technological methodology.
    - The operator is involved in implementing the technological methodology.
    - The operator is involved when using the technological methodology.
    - The operator is involved regarding the technological methodology after use.
- The **breadth** of worker participation has to be discussed (*digital twin*, *dashboards*, *allocation tool*).
    - All organisational stakeholders are involved in the development. It should be defined which ones these parties are and how they are involved (and which what interests).
    - The employee representatives should be involved proactively. They can access their rights of social dialogue in the development and regarding the outcomes.

Three remarks are added.

1. A first remark here is that there always has to be made a trade-off between excessive rates of worker participation and the examples of e.g. open-ended participation, versus getting stuck or being delayed in the project as these principles may be time-consuming, unnecessarily delaying, cause change fatigue and be costly. A saturation point of worker participation could be identified beforehand.
2. A second remark is that some choices made by worker participation may be opposite to, or even steer, methodological choices (e.g. choices for one device and no other).
3. A third remark is that operator (stakeholder) input regarding *digital twin, dashboards, and the allocation tool* has to be collected, either by means of a session or by means of integrating it in the baseline survey one way or another.

1.2 Social dialogue

- Operator well-being is a **collective concern** and should primarily be topic of social dialogue. The technological methodology should assure not to *individualise* the topic of well-being at work.
- *Digital twin*, *dashboards*, and the *allocation tool* should be used to complement; improve and by no means to replace or aggravate an organisations' well-being policy.
- *Digital twin*, *dashboards*, and the *allocation tool* should be seen as instrument that fosters social dialogue. The scope, however, should be discussed
- Existing union dynamics (broader) social relations at work need to be taken into account.
- The underlying agendas or interests (if any) of both employer and employees should be made transparent. Employee representatives may want to enforce measures based on data the tool provides. This goal-orientation may occur and should be anticipated or accounted for.
- The expected consequences may hinder participation (fear of being sued). The role of the Data Protection Authority should be recognised.

1.3 Data literacy and data awareness

- Literacy (or data literacy in particular) contends that any subject should be informed about the law. As such, ignorance is not an excuse. Operators and all other stakeholders of interest should be able to understand what the data are, which are being collected, used, generated and released.
- Awareness (or data awareness in particular) contends that any subject should know what the repercussions are of (not) abiding by the law. In case of data awareness, operators and all other stakeholders of interest must understand what the consequences of data sharing are.

1.4 Communication

- **Communication** is required to be early, timely, transparent and consistent.
- The different stakeholders should be communicated to in **different languages**, meaning that project partners should adapt their language to their interest, however, without losing the key purpose out of sight.

2 OUTCOME ETHICS

Are we reaching our goal with this methodology? The question we tackle in this section contends that whether an action is ethically right or wrong depends on the *consequences* of the action, not on the intention and the motivation. We make an estimate of the expected outcomes. In particular, we overview task rotation, user empowerment, constrained autonomy, data-facilitated harm, data-imposed, normalisation, responsibilities and accountabilities and expectations with regards to actionality.

2.1 Task rotation

- **Task rotat**ion is received with mixed reactions *(allocation tool).*
- The formulation well-being aware optimisation was received with mixed reactions.
- Ethical question 1: can we optimise group-level well-being (i.e. the cumulation of well-being of all operators) when the condition of a single operator or a group of operators worsens?
- Ethical question 2: what about an individual who has the preference to stay at his or her work station with one and the same debilitating physical task. How to balance preferences with allocation and scheduling suggestions. If we know that the consequences will improve this person's situation (consequentialism), can decide to choose for this person? And relatedly, how will this affect the person's well-being.
- Operators should be able to communicate their interests or concerns with *(allocation tool)*.
- Operators should know the root cause of their (re)allocation recommendation.
- The frequency of (re)allocating, (re)scheduling has to be discussed and considered.
- Task rotation affects well-being (see conceptual model: Bal & Dessers, 2024).
- Task rotation closely relates to function classification systems and accompanies expectations in terms of working conditions.

2.2 User empowerment?

- Operators should be able to make sense of the data they are collecting, and should be able to express themselves *about* their well-being data in a way that is easy and suitable. Especially since it comes to their well-being, a swift reply should be guaranteed. {legal principle}
- Operators will feel empowered is they can truly do something (escalate insights) based on their data. Whether something happens, however, refers to expectations and actionality.

- Operators should be enabled to personalise their own *dashboard*. Remark here is that a non-identical *dashboard* may lead to different reflections and interpretations across operators (methodologically).

- Operators should be allowed to support themselves, and follow-up their own data during the shift or during the working hours. {legal principle}

2.3 Constrained autonomy?

- Well-being data should not be used as a trigger, or, as least as possible. Using data and the *digital twin* and *dashboards as a trigger* interferes with a task execution in unvoluntary ways, and may as a consequence, increase cognitive and physical load levels (worsen well-being).

- Continuously generating well-being data may create more stress than benefiting well-being, and induce feelings of surveillance.

- Recommendations and suggestions that dashboard, and allocation tool give should be discussed, as they may affect choices and decisions operators make. This relates to the contentious concept of *nudging* in the first place and *reliance* in the second place. Both may undermine operator feelings and thoughts.

2.4 Data-imposed normalisation

- Digital twin, dashboard, and allocation tool should by no means lead to normalisation of participating in the research, nor to normalisation of well-being outcomes. {legal principle}

- Digital twin, dashboard, and allocation tool should by no means lead to data-profiling, i.e. a methodology that would work perfectly for those operators that bring forth average scores. The methodology may work perfectly for those who have average weight, average height etcetera. Key is to build the digital twin, dashboard, and allocation tool so that it is inclusive to all types of operator (physically and mentally), and that it can be employed by those who have varying degrees of well-being. {legal principle}

2.5 Data-facilitated harm

- Unintended outcomes should be proactively anticipated. {legal principle}

- Unintended outcomes that occur in situ have to be tackled or addressed. {legal principle}

- Operators' feelings of insecurity and scepticism should be taken seriously.

- Operators may by no means be discriminated or treated unfairly based on the well-being data.

- Operator well-being data may by no means be used for recruitment and retention policies.

- Operator data may by no means be misused or used against the purpose that was decided and collectively discussed.

- Operators that do not want to participate are free to do so. However, these operators could be stigmatised, socially forced, or be treated with suspicion both by colleagues (peer pressure) as well as by their team lead. {legal principle}

2.6 Responsibilities and accountabilities

- Operators may *internalise* responsibilities regarding their well-being. This is ethically a difficult one, since (1) operators are partially responsible for their own well-being (as individuals outside their workplaces), however, (2) employers and employee representatives are jointly responsible and accountable to attain to the prevention principle.
- The employer has the obligation to jointly with the representatives meet the prevention principle when it comes to operator well-being.
- The employer responsible for the complexity of decision making in the workplace, particularly when relying on technology like sensors. {legal principle}
- The employer should be aware of the potential that stress levels may increase (and of all the potential normalisation and harm risk) in the workforce. The employer should initiate means to take appropriate action to prevent harm, or should be supported in doing so.
- The employer should be aware that well-being policies cannot simply be outsourced to a tool.
- The employer should be aware that more issues may surface when rolling out this technological methodology. It may open up *Pandora's box*, so to say. The employer should be aware that well-being initiatives (and related, operators' expectations) may need a structural solution that goes beyond what the employer had anticipated. *For instance, the dashboard may reveal work stations with high physical load (as expected) and at the same time high rates of cognitive stressors due to interpersonal conflict (which was not anticipated). The follow-up may be more than ergonomic initiatives but also a social, personal coaching trajectory*.

2.7 Expectations and actionality

- It should be clarified what operators can(not) expect in terms of their situation. {legal principle}
- Operators clearly need to know beforehand what the goal and purpose is (and preferably participate in delineating this).
- Operators and their representatives need to know (and shape) how their contributions in terms of data will be used, followed up, and what will come out. There is a general frustration when it comes to *purposeless* data collection.
- No clear expectations and lacking actions will affect the credibility of the operators and will cause drop out in terms of project participation (methodologically).

3 LEGAL PRINCIPLES

Are we legally sound? Project partners should distinguish what is legally possible from what is ethically desirable. Project partners and all organisational and non-organisational parties should be aware that legal frameworks provide the absolute minimum criteria. Properly implementing technological methodology would not only mean to abide by the law, but to substantially surpass the law.

3.1 The principle of legitimacy

Personal data should be collected voluntarily, processed *fairly* and for *legitimate purposes*, i.e. only for reasons that are directly relevant to the employee (GDPR, Art. 6; ECOWAS Data Protection Act, Art. 23).

- Operators should be able to participate voluntarily. {legal and methodological principle}
- Operators should be able to withdraw voluntarily. {legal and methodological principle}
- Project partners, organisational parties and stakeholders should be aware that voluntariness is never entirely guaranteed seeing the nature of the employment contract. Representatives need to watch over this. {legal and methodological principle}
    - The *informed consent* refers to an active expression of will.
    - The *informed consent* should be given in a meaningful way. It should enable the operator to differentiate between different data types if applicable. More so, at each moment in time the operator should be entitled to stop. {legal and methodological principle}
- The *purpose* of the methodology (*digital twin, dashboard, and allocation tool*) should be limited and should not adapted over time, unless upon information and consultation with operators and their representatives.
- The *storage* of the well-being data collected need to remain relevant. Data cannot be processed for 'longer than is necessary', given the purposes (GDPR, Art. 5, 1).
- Well-being data should be stored locally.

3.2 The principle of proportionality

- The data collected should be:
    - … suitable to pursue the purpose (GDPR, Art. 5, 1);
    - … necessary and minimised (EWP, Opinion 8/2001; GDPR Art. 25, 2);

- … non-excessive (ILO Code of Practice, section 6, 14). Excessive monitoring may have a psychological impact. Even when both legally and ethically sound, operators may still experience stress or anxiety, that may unfavourably affect their well-being {M}

- The employer has no right to measure disproportionally beyond the scope of what is necessary.

- The employer has the right to conduct surveillance to a certain extent, that is when it comes to assessing the performance and the productivity of the operator. Essentially, the employment contract allows the employer to measure whether wages are worth the money. Historically, the authority to surveil was limited to the production area of a dedicated manager. A manager has the data on ongoing processes of his employees in order to act.

- Proportionality should be evaluated within the sector across organisations. In some, tracking and measuring is business as usual (chemical industry), whereas not in other.

- The operators may experience negative consequences of *sousveillance*, i.e. excessively control themselves, arguably leading to excessive disciplining, and feelings of uncertainty. This should be taken into account.

3.2.1 The principle of transparency

- The organisation should install a general policy of openness about developments, practices and policies with regard to operator well-being data;

- Operators have the right of being properly and periodically notified of their data, how these are processed and of the outcomes thereof (ILO Code of Practice; CoE Recommendation, 2015). As such, *digital twin, dashboards* and *allocation tool* need to be transparent on the algorithms in a way that is clear and understandable.

- The employer should not 'hide behind' a too rigid interpretation of GDPR-legislation. The data that *is* available about employees, should be transparent to the employee, and upon the approval of the latter, to the employee representatives. This way the representatives will be able to excess their right to protect operators.

- The employer may fear repercussions for sharing data, because of lacking data literacy and data awareness. And, because the Data Protection Authority is being conceived as a 'watchdog paralysing initiatives with data'.

- Operators are aware of what data is collected.

- Operators are aware of what these data are used for.

- Operators are aware of what these data *can be* used for.

3.2.2 The principle of confidentiality

- All parties that have access to well-being data are bound to a rule of confidentiality.

- This may mean anonymisation. Anonymisation refers data that is completely detached from individuals, making it impossible to trace back to specific persons. Anonymised data it is no

longer considered 'personal' under privacy legislation which is why it falls outside deeper regulations - you are not bound by obligations or extended retention periods.

- This may also mean pseudonymisation. Pseudonymisation (or encryption) involves replacing the identifiable information with pseudonyms (or in an unreadable format). In both cases, the data can still trace back to individuals if necessary, meaning the data remain 'personal'. But if it still had, you know, individualised data- just a number without being directly linked to personal data - that is pseudonymised data, but it is still considered personal data according to GDPR. Processing data (as a data controller), should be covered in the data processing agreement, especially concerning liability, ensuring that it is clearly defined and limited.

- Anonymisation and/or pseudonymisation well-being data has consequences for aggregation:

  - importantly, the employees (data subjects) and their representatives should be able or enabled to decide what can be done with their data in terms of aggregation. Do they want to share their data in pure anonymity or do they allow data to be brought back to them, and to have analyses made on their data;
  - the choice (not) to share data in an anonymised or pseudonymised way will affect the potential of the aggregated well-being scores. Systematically not accounting for operators who not want their data to be shared, will affect the overall picture. More so, it has the potential to stigmatise the ones who opt not to share the data.

3.3 The principle of access

- Operators have the right to access their well-being data (OECD Guidelines, 2013)

- Operators can do so during the working hours.

- Operators have the right to data portability (GDPR, Art. 20), i.e. '*the data subject (operator) has the right to receive his or her personal data provided to a controller, in a structured, commonly used and machine-readable way. The data subject has the right to transmit those data to another controller without hindrance from original controller'* Employees should be entitled to designate a representative who has the right to have access to their well-being data and/or be able to access them through a medical professional of their choice. Employers should not charge workers for granting access to or copying their own records.

- Operators have the right to access their data in respect of evaluation purposes. The opinion about an operator in turn is data about this employee, and should be consultable.

- Operators should clearly know who has access to the data and who has not. In case the data is treated or analysed by third parties, this should be clearly stated.

4 METHODOLOGICAL REQUIREMENTS

Are we reflecting or deflecting operator well-being? Since we are developing a technological methodology, all project partners should be aware our main purpose is to reflect (and not to deflect) well-being metrics. Taking methodological requirements seriously is a necessary precondition that precedes the other requirements.

4.1 Validity

- Validity refers to whether or how well a measure represents the construct it is expected to measure. Project partners should question how well we are capable of *reflecting* (or that we deflect) well-being.

- The project partners discuss whether they are capable of presenting an accurate depiction of operator well-being, and to what extent this depiction does or does not cover the construct of operator well-being. *For instance, is one depiction reflects 10% of operator well-being, what can and will be done with the data may differ from a depiction reflecting 90 of operator well-being.*

- This closely relates to who takes the role of the data controller and who determines the purpose and the means of data processing. {legal principle}

4.2 Datafication

- The project partners, organisational stakeholders and other parties should realise that …
  - … we tend to over-rely on numerical data, expressions and explanations to make sense of the empirical reality, i.e. that we are only relying on data to make sense of operator well-being;
  - … making statements based on 'objective data' not simply increases the *manageability* of operator well-being;
  - … integrally objectifying well-being is a difficult undertaking;
  - … objectifiable or objectified data is often treated as authorised knowledge and that objectifiable data should be seen as an indication of operator well-being, and not as the reality of operator well-being;
  - … researchers tend to appreciate correlation over meaningful causation.

- Datafication has been said to draw away the attention from what is at stake (i.e. operator well-being) by simply looking at the data. Obtaining good well-being data may in that sense become an extrinsic motivator, that draws away the attention from well-being itself. On the other hand, datafication may also create more awareness of the well-being issues at hand.

- Datafication risks to make use of *arbitrary thresholds and standards*.

4.3 Reliability

- The measurement of data should be reliable, consistent, repeatable when measured. In the context of data protection legislation 'data quality' is formulated as a reference to reliability. {legal principle}

4.4 Manipulation and modification

- Data manipulation refers to the intentional and conscious alteration or modification of data collected. Data manipulation in that sense closely relates to reliability as it is a conscious act not to be reliable and occurs when employees know which specific metrics are being measured and how the consequences of these measurements affect their conditions.
- Operators have the right to modify or rectify their data by law (GDPR, Art. 16). {legal principle}
- Operators have the right to have their data deleted.
- Operators have, in this context, the right to lie without termination of the employment contract (ILO Code of Practice). Generally speaking, lying has only been grounded as 'defensive' and therefore permissible right as a way to avoid (impermissible) wrongdoing.
- The event of operators *manipulating* well-being data should be taken seriously. If employees come to learn what data entry (either via micro-survey or via sensor technologies) will result in particular outcomes, they may alter their survey responses or their sensor measurements to influence the outcomes of the algorithm.

4.5 Data interpretability

- Operators should be able to interpret their own well-being data via the *dashboard*.
- Operators should be able to make sense of the various graphs in real-time.
- Operators should be able to make sense of the various graphs over time.
- Operators should be open to reflect about their own data with a third party.
- Operators should be entitled immediate feedback upon request seeing the topic of well-being.
- Operators should be able to interpret their data with whomever they feel suited (portability).
- Operators may require interpretative support when it comes to support in making sense of the data.
- Operators may require psychological support when it comes to positioning their data.

- Operators have the right to have their own subjective interpretation of the data.

4.6 Data reactivity

Data reactivity refers to changes in employee behaviour, attitudes or feelings due to the act or the repeated nature of the self-monitoring, potentially biasing the data collection.

- The mere fact that operators are using this technological methodology may in itself affect their well-being.
- The rate of intrusiveness is likely to affect the rate of data reactivity.

4.7 Data inference

Data inference in this study involves drawing conclusions or making generalisations about one operator well-being based on data collected from this operator.

- Project partners should evaluate the quality of the data is data points are missing.
- Project partners should evaluate what systematically missing values mean.

4.8 Data aggregation and participation bias

Data aggregation refers to the capability to present anonymised or pseudonymised data at a higher hierarchical level of organising. Data aggregation in itself should be questioned and positioned to the purpose of the different initiatives *digital twin*, *dashboard,* and *allocation tool*.

- Project partners realise that operators systematically opting out of data collection will (heavily) influence the conclusions drawn at a more aggregate level.
- Project partners should evaluate the potentiality of drawing conclusions at an aggregate level, the overall and aggregate picture should by no means be able to lead back to or identity single operators.
- Participation bias may occur, i.e. non-response bias in which the results or aggregate results become non-representative because certain respondents (operators) systematically drop out.
- Project partners should evaluate the ability to aggregate and disaggregate well-being data. In combination with the limitations of data inference (some individuals systematically dropping out of participation), aggregating systematically incomplete data may be ethically not sound. *For example, if higher-level overall picture shows two teams are excelling whereas two teams are scoring less in terms of well-being, and additionally, certain people in the latter two teams are systematically not participating, stigma may arise and conclusions may be drawn.*

4.9 Technological feasibility and intrusiveness

- Project partners should provide an integrated technological methodology so that operators want to work with it.
- Project partners should realise that one technology in itself may be imposing and intrusive, let alone the cumulation of several different technologies.
- Project partners realise that some technologies request the use of personal devices, e.g. do visualise scores, etc., which may have advantages and disadvantages.
- Project partners realise there are issues with certain sensor technologies in terms of reliability. The technology should at re*allocation tool* be evaluated in terms of accuracy and reliability of the data it provides.
- Project partners realise that the effectiveness of certain sensor technologies may be influenced by person related characteristics, e.g. skin tone, body weight, etc.

GENERAL CONCLUSION

This report has highlighted the ethical and privacy challenges that arise when developing technologies for continuous monitoring of operator well-being. By combining insights from academic literature and interviews with experts and stakeholders, we identified key concerns. These findings were translated into concrete design requirements to ensure that the WellFiciency methodology is not only technically robust, but also ethically sound and socially acceptable. Embedding these requirements from the outset will be essential to foster trust, support adoption in industrial settings, and promote the responsible use of well-being data in the workplace.