


Università Ca'Foscari Venezia

UNIVERSITÄT HOHENHEIM

Master's Degree

in Management

Final Thesis

Balancing Wearables in the Workplace: Protecting Privacy and Human Rights - a Legal Analysis within the European Legal Framework

Graduand

Eileen Plogsties

893882

Supervisor

Professor Vania Brino

Academic Year

2022/2023

to obtain the Double Degree in Management between

Universitá Ca'Foscari di Venezia and University of Hohenheim

Hamburg, September 2023

Abstract

Digitalisation is transforming the current work environment. With the incorporation of new technologies in the workplace arise challenges especially regarding privacy and human rights. Since wearables and Internet of Things (IoT) devices are becoming increasingly important for business operations, the analysis focuses on the privacy and human rights implications arising from the incorporation of wearables in the workplace. Specifically, an elaborate legal analysis of the current EU regulatory framework to examine the effectiveness in addressing the privacy and human rights challenges was conducted. The General Data Protection Regulation (GDPR) is examined in detail and complemented by other relevant regulations and directives aimed at mitigating privacy concerns, as well as the European Convention on Human Rights. Germany's approach will be presented as an example to demonstrate the implementation of the European legislation based on a case study.

The analysis reveals that while the European legal framework is notably robust in terms of protecting personal data, significant gaps remain in ensuring privacy and upholding the human rights when implementing wearables in the workplace. These gaps include issues related to employee consent, liability, transparency, and the potential violation of human rights, like the right to equality and the right to non-discrimination. A balance between legal, technical, and ethical considerations is essential to protect the rights of employees.

In response to these challenges, this study proposes solutions that aim to balance ethical and technical aspects and address legal issues. A multi-stakeholder approach is proposed, which provides an outlook and aims to improve the legal framework to effectively address the complex challenges posed by the integration of wearables in the workplace. Finally, factors that promote the successful adaptation of wearables in the workplace are presented. These factors include a strong regulatory framework, a balanced assessment of potential risks and benefits, the integration of the technology into the company's overall business strategy and the establishment of collaborations.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

IoT	Internet of Things
GDPR	General Data Protection Regulation
AI	Artificial Intelligence
EU	European Union
AR	Augmented Reality
ECHR	European Convention of Human Rights
CFR	EU Charter of Fundamental Rights
OSH	Occupational Safety and Health
PPE	Personal Protective Equipment
IGO	Interorganisational Organisation
ILO	International Labour Organisation
WTD	Working Time Directive
AI Act	Artificial Intelligence Act
PLD	Product Liability Directive
TPWCD	Transparent and Predictable Working Conditions Directive
CSDDD	Corporate Sustainability Due Diligence
CSR	Corporate Social Responsibility
PIA	Privacy Impact Assessment
AGG	General Treatment Act

1 Introduction

Digital transformation is reshaping the workplace (Lamarre et al. 2023). Companies face the challenge of remaining competitive by mastering new technologies and integrating them effectively into their business operations. Specifically, wearables and Internet of Things (IoT) devices, are gaining popularity because of their beneficial implications for performance and workplace safety (Eager et al. 2020; Maltseva 2020). Wristbands, headbands, smartwatches and glasses are examples of current workplace wearables (Maltseva 2020). Wearable technology can be capable of Artificial Intelligence (AI) and may interact with systems that are driven by AI which extends the implications arising from the implementation in the workplace (Moßner and Bergmann 2019). As a result of the extensive collection and analysis of personal data by these technologies, challenges arise regarding the protection of employees' privacy and human rights (Patel et al. 2022). Therefore, the following analysis focuses on the privacy and human rights implications when incorporating wearable devices into the workplace. Mitigating risks and reducing potential negative impacts on employees are critical for companies, not only in terms of compliance, but also to ensure increased performance and successful technology integration (Mettler and Wulf 2019; Miele and Tirabeni 2020; Lamarre et al. 2023). Hence, balancing risks and opportunities when implementing wearable technology in the workplace is essential, to reduce inferences with employees' rights and maintain positive impact from wearables on performance and workplace safety.

In the following, a legal analysis will examine the current European legal framework for the protection of privacy and human rights in the context of wearables. The study aims to elaborate whether the current legislation is sufficient to protect employees' rights in times of rapidly evolving technologies. The focus of the analysis will be the legal framework of the European Union (EU), since it is a pioneer in protecting privacy and personal data (European Comission). As the main data protection law in the EU, the General Data Protection Regulation (GDPR) is examined in detail and complemented by other relevant regulations and directives aimed at mitigating privacy concerns. The study also focuses on the human rights implications set out in the European Convention on Human Rights. Therefore, the study aims to answer the research questions whether the legal framework covers all potential privacy and human rights risks that arise from implementing wearables in the workplace.

Germany’s approach will be presented as an example for assessing the implementation of EU regulations into a national legal framework. The case study will highlight the current privacy and human rights legislation in Germany to draw conclusions on potential improvements.

The study concludes by outlining the remaining legal, technical, and ethical challenges. A prospective framework attempts to address these challenges by promoting a multi-stakeholder approach. Moreover, the research identifies several factors that support the successful integration of wearables in the workplace.

Finally, this study will summarize the main findings and address the research questions. The limitations of the research will also be discussed, along with potential areas for future research. Finally, a personal evaluation will be provided.

2 Balancing Wearables in the Workplace: Privacy and Human Rights

The work environment is undergoing a transformation due to the increasing integration of wearable technology (Stefano and Wouters 2022). To achieve a broad understanding of the concrete implications, risks and opportunities of wearables in the workplace, the nature of what wearables are, the data they collect and their integration into work environments will be explored. Establishing a common theoretical understanding of the concepts of privacy and human rights is crucial to provide a solid basis for further legal analysis. The study will then examine the opportunities and risks arising from the use of wearables, with a particular focus on balancing privacy vs. performance and monitoring vs. autonomy as a human right. A conceptual model presents this impact of wearable technology in the workplace and shows how the legal framework for protecting employees' privacy and human rights comes into play. The model also highlights the fact that the integration of wearable technology involves numerous stakeholders with different interests such as the business, government, and employees.

2.1 Key Concepts

In the following, the key concepts and scope for the thesis of “wearables”, “privacy” and “human rights” are defined to get a mutual understanding and set the basis for further analysis.

2.1.1 Wearables in the Workplace

The term wearable stands for “an item that can be worn” (Oxford Dictionary 2023). Wearable technologies are small, networked computing devices delivering personal and sensitive data about the user by being worn or attached to the body (Ching and Singh 2016). Wearables can be associated to AI but are not limited to it. However, it is important to note that wearables in general do not exclusively belong to AI, since not all wearable devices have the capability to connect to AI tools (Moßner and Bergmann 2019). In the analysis wearables are considered to be part of AI as they may interact with systems that are driven by it. The reciprocal effects of wearables and AI and therefore the growing opportunities as well as risks are part of the analysis.

Attaching wearables to the human body and collecting sensitive data about individuals not only raises legal challenges concerning technologies but also raises legal considerations related to human rights.

Wearables appear in forms as smart-watches, wristband, or glasses but can take on a number of different shapes as well (Federal Office for Information Security Germany 2023). The device may be capable of measuring heart rate, blood pressure, sleep and calorie consumption, among other things, and then have the measurement results evaluated via AI applications to take assumptions about health status or productivity of the wearer (Federal Office for Information Security Germany 2023). These AI applications analyse the data and are capable of taking automated decisions for the user (Raso et al. 2018). The data collected can provide critical information for employees and employers to generate safer working conditions or prevent workers from negative long-term health consequences. Wearables that monitor the health and well-being of employees can indirectly increase efficiency by ensuring that employees are healthy and able to perform optimally. Early detection of fatigue or stress can lead to necessary breaks or adjustments in workload. Further, wearables can be integrated into workflows to optimise processes. For instance, in manufacturing or logistics, wearables can provide step-by-step instructions, reducing errors and minimizing the time taken to complete tasks.

Wearable Devices can be embedded into an IoT ecosystem like an app to make the measured data visible and easier accessible for the user (Ching and Singh 2016). IoT refers to a system of interconnected machines and devices via and with the Internet. The "things" connected to it must be clearly identifiable (Moßner and Bergmann 2019). IoT platforms offer the opportunity to connect amongst the wearables and their app a variety of other applications and tools that they can interact and exchange data with (Moßner and Bergmann 2019).

The technology is characterized by being always-on and continuously collecting data about their environment. It integrates seamlessly into a network of other devices, operates hands-free and has its own operating system. To attract the user's attention when intervention is required, it communicates through vibrations or sounds (Ching and Singh 2016).

Wearables are being increasingly integrated into the workplace in several ways. The most common application involves monitoring employees' stress levels, behaviour, and performance, as highlighted by Khakurel et al. (2017). These wearables serve as valuable tools to assess and manage employee well-being (Khakurel et al. 2017).
Additionally, wearables are utilized as external tools to assist with tasks such as lifting heavy items, adjusting posture, and tracking employees' positions and movements.

These devices contribute to improving workplace ergonomics and promoting employee safety (Patel et al. 2022).

Another application involves the use of augmented reality (AR) wearables, which connect digital information with the real world. These wearables usually consist of glasses or headsets that are equipped with displays, cameras, sensors and processing functions to create an augmented reality experience (Hackl 2023). By integrating digital content within the physical world, these wearables increase productivity and are an enabler for greater efficiency. These types of wearables commonly utilize artificial intelligence (Hong 2013).

Furthermore, Wearable devices can continuously monitor employees' activities and provide real-time data on their performance, productivity, and health. This immediate feedback enables quick adjustments and optimisations that ultimately improve overall efficiency (Maltseva 2020). Importantly, these utilization options are not mutually exclusive, and wearables can serve multiple functions simultaneously (Khakurel et al. 2017).

However, it is to be noted that different industries require different solutions to tackle the posed risks and hazards at the workplace and optimise their working equipment. A sedentary job such as an office job must deal with the negative effects of sitting such as neck and back pain, while hearing problems are more likely to occur in industries with high noise exposure such as construction. This is why usage and exposure of wearable technologies varies from industry to industry.

The different types of wearables can be categorized according to their application in the work environment monitoring workplace safety, employee well-being, and performance (see Table 1).

Wearable Technology	Application	Workplace/ Industry	Impact
ErgoSkeloton	Adjusting posture and assist heavy lifting	e.g. manufacturing, wearhouses	Employee well-being, workplace safety
SmartCap LifeBand (band attached to a helmet)	Tracking fatigue level and alertness	e.g. manufacturing, transportation	Employee well-being, workplace safety
Smartwatches (Apple Watch, FitBit)	Tracking steps and stress level, heart rate etc.	e.g. sedentary jobs	Performance, employee well-being
Smart Glasses, AR-Headsets (AI capable)	Tracking movements and employee location, visual instruction	e.g. wearhouses	Performance, automated decisions

Table 1 Overview of Wearables Application in the Workplace

Wearable technologies that monitor workplace safety, such as those that indicate or support heavy lifting, respond to hazards, identify dangers or fatigue risks and detect stress, constitute one category (Patel et al. 2022). Examples of wearable devices that address these safety risks include the StrongArm ErgoSkeloton Lift, which transfers the load from the upper body to the legs and assist workers with heavy lifting and therefore reduce strain on the back (see Figure 2-1). Another example is the SmartCap LifeBand which uses sensors and brain waves to measure fatigue and alertness in real time (see Figure 2-1). The information can be transmitted and displayed in the connected LifeApp (Patel et al. 2022). The IoT solution Kenzen's app, patch and monitor, so called Personal Protective Equipment (PPE), tracks heart rate, stress, and temperature with biosensors integrated into the patch to report stress, heat assessment, and exercise.

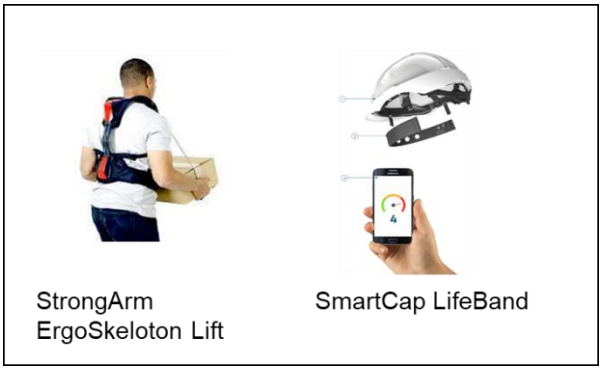


Figure 2-1 Wearables for Workplace Safety

Wearable devices designed for monitoring employee well-being play a crucial role in mitigating health risks for workers. By continuously monitor physical activity they enable detection of potential hazards such as work-related musculoskeletal disorders, functional movement disorders, and work-related pulmonary and cardiovascular diseases. Additionally, these devices can provide indications for occupational sun protection, and therefore ensure employee well-being (Patel et al. 2022). Popular examples of such wearables include smartwatches and activity trackers like the Apple Watch or FitBit, which record measures like activity levels, sleep patterns, heart rate, and respiration (see Figure 2-2).

Additionally, there are special devices that prioritise employee well-being, such as a clip-on device and its accompanying app that records UV exposure and vitamin D

production. Those specific devices help employees monitor their sun exposure and maintain adequate vitamin D levels.

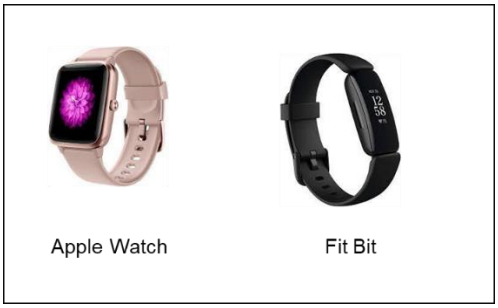


Figure 2-2 Wearables for Employee Health

In addition to health monitoring, wearables can also be used to monitor performance in form of productivity in the workplace. Through monitoring social behaviour, implementation of augmented and virtual reality technologies, motion control, and stress management it can give assumptions about performance. Smart glasses or AR headsets are commonly used in various industries to provide visual instructions or 3D mapping for improved orientation.

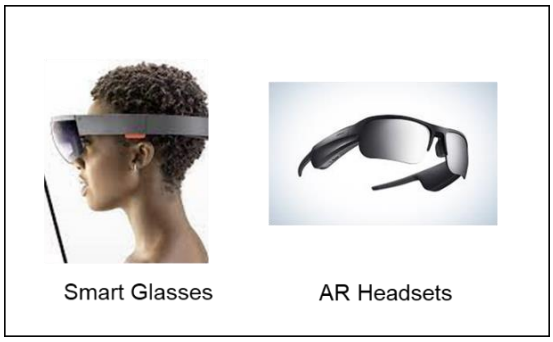


Figure 2-3 Wearables for Productivity

Wearables are collecting different kind of data. They can be categorized into raw and processed data (Maltseva 2020). The data can be processed from the wearable or in later processing steps from AI applications. Raw data has not been processed and has only been gathered for example the number of steps taken. Processed data has been analysed to be able to take assumptions about employee well-being or performance. For example, heart-rate variability leading to an evaluation of stress-level (Maltseva 2020). The processed data is often analysed and visible on a monitor or smartphone connected to the computing device. Generally, the data can be classified as sensitive since the personal data collected are genetic and health-related data

(European Comission 2023d). Therefore, a high level of information security is critical to protect unauthorised access to that sensitive information because it can cause loss of security and privacy and can harm businesses or individuals and their human rights (European Comission 2023d). That means specific processes are required to store and use the data to meet the requirements of data protection laws.

Wearables collect data that offer valuable insights into a user's real-life actions and habits, going beyond the scope of job performance evaluation. This distinguishes it from traditional monitoring methods or self-reported assessments of employee behaviour, which primarily rely on subjective performance indicator (Maltseva 2020). These indicators are based on employees' perceptions of their own productivity improvements and not on objective measures or data.

The adoption of wearables in the workplace is transforming the work environment by changing existing job roles, working conditions and performance. However, these changes are also giving rise to inequalities in the workplace and in the job market. Therefore, the incorporation of wearables carries the potential to impact human rights significantly (Raso et al. 2018).

To conclude, wearables at the workplace enable monitoring of individual employees' activity, behaviour, and physical condition. Examples are smart and on-body accessories and personal protective equipment. These technologies are often complemented or embedded into an IoT ecosystem to extract information and analyse data in order to enhance workflow and/or time management. The integration of wearables into business operations aims to monitor and improve employee safety, well-being, and performance as well as organisational performance. However, integrating wearables may have consequences for employee privacy and human rights since it involves the collection of personal data and changes the dynamics of the workplace.

2.1.2 Privacy

When it comes to developing and integrating wearable technology in the workplace, privacy of the employee is a focus topic of ongoing research (Wolf et al. 2016; Psychoula et al. 2020). The concept of privacy is complex and it challenges the scholars to define its nature properly (Albakjaji and Kasabi 2021; Kokolakis 2017). Amongst various definitions the main characteristics that stand out are, that privacy is both a

social value and an inherent human right (Segura Anaya et al. 2018; Karale 2021; Brey 2007).

Privacy is a non-public and non-tangible sphere surrounding a person in which it perceives freedom and control over its personal live (IAPP 2023). The concept privacy involves the ethical evaluation of human behaviour and interactions and how is it aligned with social values, safeguarding individuals' personal lives and personal information (Brey 2007).

In the European Union the law considers privacy as part of the basic human rights (ECHR 2023). Privacy is the fundamental human right to keep personal information by themselves without interference (IAPP 2023). It involves the right for autonomy, the control over personal information and the right to be let alone (European Union 2023). Through interaction with people, talks and discussion with others we share information about our lives and let them in to our privacy sphere. We can decide how much we share from our personal live and how much we give away from our privacy. The extent of our connection and relationship with another individual determines the quantity and detail of information we disclose. For instance, we share more private information with friends as opposed to colleagues.

Part of a person's privacy is personally identifiable data consisting of information about our personal lives and characteristics that make one as an individual unique (European Comission 2023d). This type of data contains confidential information about the person so that they can be identified. Personal data involves name, date of birth, address but also health data or biometric information (European Union 2023).

Data protection is the right to decide, throughout the data processing cycle, who can access data and for what purpose it is collected (European Union 2023). The collection of sensitive health data through wearable technology underscores the critical importance of personal data security in ensuring privacy. Therefore, it is essential to prevent the processing of personal data from leading to vulnerabilities that undermine privacy. This results in the need to create technical conditions to ensure data protection and therefore privacy in the workplace (Segura Anaya et al. 2018). Data protection aims to secure personal information which is crucial in terms of wearable technology that collect and analyse personal data (European Data Protection Supervisor 2023). Privacy and data protection rights are strongly linked, especially in the context of technology, but they are two distinct rights (European Data Protection Supervisor 2023).

However, in the following analysis, the right to data protection is considered as part of the overall concept of privacy. The term “data protection” is sometimes named data privacy outside of Europe (European Union 2023).

The legal ground aims to make the construct of privacy tangible and to protect privacy and personal data. The right to privacy and the right to data protection are embedded in the primary law (European Comission 2023b). Therefore it is the basis for the rules, decisions and the following secondary law in the EU including regulations and directives (European Comission 2023c).

The right of privacy is a human right and therefore part of the Universal Declaration of Human Rights (Article 12), the European Charter of Fundamental Rights (Article 7) and the European Convention of Human Rights (Article 8). The right to data protection is crucial to secure privacy and is part of EU Treaties but not a human right itself. The protection of personal data is enshrined in the EU Charter of Fundamental Rights (Article 8) and established through the General Data Protection Regulation, an independent EU regulation (European Data Protection Supervisor 2023).

Within the European Union, privacy and data protection are not considered as absolute rights and can be limited under specific conditions. In some cases, these rights may require a balance with other EU values and rights (European Data Protection Supervisor 2023). As an illustration, the EU is actively driving regulatory advancements in this field of technology through initiatives like the EU's Data Protection Regulation (Latonero 2018).

2.1.3 Human Rights

According to the Scholars, the literature captures privacy as a social value and a human right closely connected to the right of data protection. We have clarified the concept of privacy as a social value and how it relates to data protection. Elaborating on the human right is now vital to the upcoming analysis and exploration of the assessment of human rights legislation outlined in chapter 3.2.
To begin with, the term human rights and the legal framework around it will be explained, and which human rights may be affected by wearable technology will be outlined.

Human rights are universal rights that are “inherent in all human being” (United Nations 2023). That means they are held by everyone simply by being a human. All human

beings are entitled to these rights including right to liberty and security, freedom of speech, freedom from discrimination and right to privacy (United Nations 2023). The human rights principles are protected and cannot be waived and stand above any other law.

The first official recognition of written human rights occurred on December 10 in 1948, with the adoption of the Universal Declaration of Human Rights by the United Nations General Assembly (United Nation General Assembly 1948). This declaration continues to significantly shape the development of international human rights law (Moeckli et al. 2022). To give the human rights formulated in the Universal Declaration legally binding force at the international level, the Declaration of Human Rights and two additional protocols were amended to create the International Bill of Human Rights (United Nations 2023). Important for further analysis is the coverage of human rights particularly in the European Politics. The Declaration of Human Rights documents and human rights principles are relevant and incorporated in the EU Charter of Fundamental Rights (CFR), which works together with the European Convention on Human Rights (ECHR) to protect the human rights in the European Union (ECHR 2023).

The Human Rights Principles are not directly legally binding but serve as a guidance how to apply human rights standards into business activities. They provide insides on how companies can incorporate technologies and implement due diligence processes to identify and mitigate potential threats to human rights (Raso et al. 2018).

The human rights principles relevant in context of wearable technology are the following (European Court of Human Rights 9/3/1953; European Parliament 12/1/2009). The concrete implications will be analysed in chapter 3.2:

- right to equality and right to no discrimination (ECHR, Article 14; CFR, 15, 20)
- right to work and right to protection against unemployment and right to have favourable conditions at work (CFR, Article 15, 31)
- right to privacy and data protection (ECHR, 8; CFR, Article 8)
- access to justice and right to fair trial (ECHR, Article 6)
- right to freedom and security (ECHR, Article 5; CFR, Article 6)

To summarize the human rights are universal to all human beings. They are laid down in the European legal framework in the European Charter of Fundamental Rights and

the European Convention of Human Rights. The consideration of human rights is of key importance in this paper, as the use of wearable technology involves personal data processing which falls within the scope of the right of privacy which is a human right. The human right principles outlined in the European Convention of Human Rights form the basis for the analysis presented in chapter 3.2, which examines the impact of wearable technology on human rights in the workplace within the European legal framework.

2.2 Balancing Risks and Opportunities

The incorporation of wearable devices in the work environment presents opportunities and risks that encompass both individual and organisational levels, as well as technological and social aspects. Balancing the risks and opportunities of wearables in the workplace requires several aspects to be considered and decisions to be made. This involves balancing the increase in monitoring activities, which can reduce employee autonomy and individual freedom, with the need to increase productivity while also increasing privacy risks. This emphasizes the impact of wearables technologies in the workplace, namely on privacy and human rights such as autonomy. This underscores the necessity of a legal analysis to assess whether the legal framework offers sufficient protection for the employee's right to privacy and human rights.

2.2.1 Balancing Monitoring vs. Autonomy

Wearables and connected AI systems can automate many of the tasks involved in employee monitoring, increasing workplace safety and health, reducing the workload on managers, or supporting them in decisions. Wearables as a monitoring instrument can be beneficial in terms of security, productivity, and efficiency (Maltseva 2020; Patel et al. 2022). Yet, the monitoring can reduce employee’s autonomy of structuring their work tasks and may restrict perceived individual freedom (Maltseva 2020). Therefore, it is important for companies to find an equilibrium between implementing wearable technology to monitor employees and mainly their security and health and maintaining individual autonomy and freedom as a human right.

The integration of emerging technologies like wearables in the workplace can positively impact employees and their work conditions. Incorporating wearables successfully can lead to a higher workplace safety by raising awareness and recognition of work-related issues (Mettler and Wulf 2019; Eager et al. 2020). These devices can alert and protect

employees in dangerous situations, leading to a safer work environment. The device has the ability to anticipate health risks that can affect employee performance and workplace safety, such as stress (Han et al. 2017), sedentary behaviour and physical inactivity (O'Keeffe et al. 2020), or even collaborate with other AI tools to identify symptoms of depression (Abd-Alrazaq et al. 2023) and heavy lifting (Patel et al. 2022). This allows the employee to adjust breaks, thereby reducing occupational incidents resulting from fatigue and inattention. The device can assist or alert the user before they suffer the consequences of harmful behaviour and can therefore lead to improved well-being of employees. Increased employee well-being at work also influences the workplace safety positively (Mettler and Wulf 2019).

Moreover, wearables have the potential to not only prevent health risks imposed at the workplace but promoting a culture of well-being as it can motivate employees to life more active and aware of their health even outside of their workplace (Maltseva 2020). By offering continuous monitoring and timely reminders, the wearable function as a proactive tool that encourages individuals to live more health conscious. For example, after a period of inactivity, the device reminds the user to move to avoid negative effects of being sedentary and can thus serve as an incentive to move and avoid sitting for long periods (Li et al. 2016).

Additionally, wearables can also support compliance with group norms and values within the organisation, as highlighted by Mettler and Wulf (2019). The devices can play a role in reinforcing and aligning employees' behaviours with the desired organisational culture and values (Mettler and Wulf 2019). These values encompass an active lifestyle and a dynamic work environment, demonstrating that employee health and well-being hold a high importance.

While the integration of such emerging technology in the workplace offers opportunities regarding employee monitoring, it is important to recognise that it also brings potential risks and challenges in terms of maintaining employee’s autonomy.

Introducing wearables at work can restrict employees’ freedom in terms of structuring and organizing their work tasks and activities (Mettler and Wulf 2019). This risk arises because data generated by the devices may draw conclusions about the optimal break times based on the employee's fatigue and stress levels and suggest more efficient process flows. Consequently, the use of wearables could introduce external influence

and guidance that could constrain the autonomy of employees in managing their work. (Mettler and Wulf 2019).

Monitoring through technology and a more technologized workplace in general not only affect employee well-being but also their motivation and engagement. Constant monitoring can lead to employees finding their work less meaningful which can lower motivation and hindering creative processes such as innovations and therefore limiting their perceived freedom (Stein et al. 2019).

Wearables offer the opportunity to quantify performance and set standards which helps companies to regulate and evaluate their employees. However, this may lead to increased power imbalances between employers and employees, which negatively impacts engagement as individuals may feel undervalued (Maltseva 2020). Wearables allow employers to constantly monitor their employees in the workplace. This constant surveillance can create an atmosphere where employees feel a lack of privacy and may restrain their behaviour, potentially creating an imbalance of power in favour of the employer.

Quantifying job performance is difficult since different settings and environmental conditions require certain skills, capabilities and employee behaviour that cannot be constrict into general measures, for instance to measure the time for a task to track employee performance can overlook several factors influencing the complexity of productivity (Abd-Alrazaq et al. 2023). It further decreases individual autonomy and freedom regarding the work tasks.

Another aspect is the potential overreliance on technology that can bring up questions about responsibility and liability in case of failures (Mettler and Wulf 2019). It may lead to decreased employee awareness and a tendency to uncritically trust the results and reliability of information collected and analysed by the device. Thus, leading to lower understanding of one’s abilities and the tasks being performed and eventually creates a less-human centred work environment. A less human workplace, or so-called dehumanisation of the workplace, can have a negative impact on employee well-being and can also negatively affect cognitive processes (Maltseva 2020). This corresponds with reduced perceived autonomy.

2.2.2 Balancing Performance vs. Privacy

Wearable devices can positively impact productivity and individual performance through constant feedback on their performance (Miele and Tirabeni 2020). This constant monitoring promotes awareness and gives an extrinsic motivation for employees to strive for higher levels of productivity. On the other hand, the constant data analysing of personal data may violate the private sphere of the employee.

Wearables have the potential to positively impact employee engagement and organisational performance (Eager et al. 2020; Miele and Tirabeni 2020). By incorporating these devices to monitor the activity of employees and integrating them into a corporate health initiative, businesses can advance employee involvement with the organisation. For instance, rewarding employees for achieving specific targets, such as 10,000 steps per day. This approach encourages employees to actively participate in wellness initiatives and can lead to higher involvement with work and commitment to the organisation.

Moreover, wearables can facilitate efficiency and process optimisation by analysing the data they collect in the workplace (Miele and Tirabeni 2020). Improved product quality and reduced production failures can enhance efficiency and decrease costs.

Finally, the data collected by wearables can help supervisors and managers in supporting their team and individual employees (Miele and Tirabeni 2020). The data gives valuable insights which can help to adjust optimal break times or more individualized support to employees. This can significantly enhance employee performance and therefore organisational performance.

While the integration of wearables in the workplace may benefit productivity and performance, it is crucial to understand the trade-offs. It also presents potential privacy risks and challenges of data protection analysing such personal data of the employee to increase performance.

Surveillance in the workplace by wearables poses risks to employee well-being, motivation, and privacy (Safavi and Shukur 2014; Motti and Caine 2015; Maltseva 2020; Miele and Tirabeni 2020). Since monitoring tools are constantly collecting data about the employee, the data collection and data analysis is vulnerable to threats posed by external and internal parties. The instant and continuous data collection does not end after working hours or after leaving the workplace if the wearable is still worn on or

detached to the body. This can lead to a blurring of the lines to employee's private sphere, since the data could be used to determine work performance (Maltseva 2020).

Furthermore, the wearable device itself presents risks to secure employees' data and its privacy. The current challenges associated with these devices include authentication issues and insufficiently secure PIN systems, which may allow unauthorised access by third parties without the users' knowledge (Safavi and Shukur 2014). Wearables have the capability to track an individual's location and activities, which could be used for marketing purposes. Further, if location data is accessed by unauthorised third-parties, employees may be at risk of physical harm, especially if they can be tracked to their homes or other personal locations (Federal Office for Information Security Germany 2023). Third party access also raises concerns about the possibility of recording videos or images without the consent of the user (Safavi and Shukur 2014).

Moreover, the data collected is descriptive in nature and does not reveal causal relationships, so careful analysis and interpretation of the data is necessary to avoid analysing data out of context (Maltseva 2020).

The data collected by wearables presents potential risks. The sensitive health data can provide insights into employees' abilities, such as stress management, and could be used by managers to favour or discriminate against employees based on their physical data (Maltseva 2020). The collection and storage of personal, confidential and sensitive data by wearable devices is causing concerns among users regarding their privacy (Motti and Caine 2015).

To ensure the security and privacy of sensitive information, it is essential to encrypt the data transmission from wearables to connected mobile devices via Bluetooth, thereby deidentifying the data. Many wearables do not use encryption during data transfer, and thus, posing significant privacy risks (Ching and Singh 2016). Not only the data transfer from the wearable to the local device, but the connection from the mobile device to a cloud storage via Wi-Fi presents security risks which makes them vulnerable to hacking or unauthorised access by third parties. In addition, a non-secure cloud storage can lead to a safety hazard since it contains a huge amount of personal identifiable information (Ching and Singh 2016).

Throughout the data collection, analysis, storage, and transmission process within the IoT ecosystem of wearables, several potential risks arise that can violate employee privacy.

Lastly, the physical loss of the wearable or local device presents a security risk because the data stored on the device is also lost (Ching and Singh 2016).

2.3 Conceptual Model

The following conceptual model illustrates the balancing of interests between the beneficial effects of wearable technology like performance enhancement and the monitoring opportunities and the impact on employees, namely on privacy and human rights when introducing wearable technology in the workplace. The model seeks to point out the interplay between wearable technology, privacy, and human rights and all the involved stakeholders.

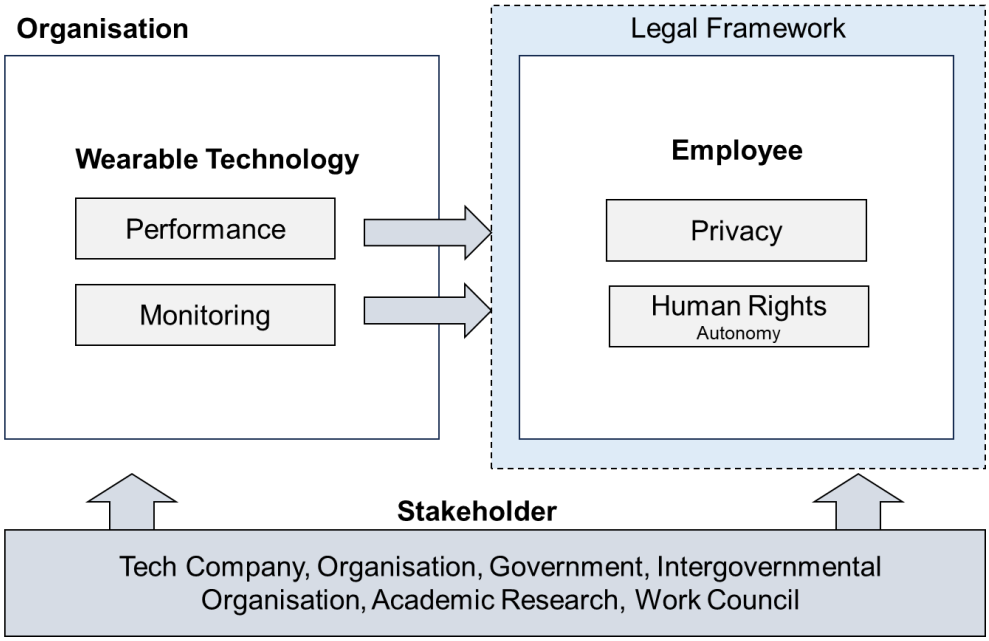


Figure 2-4 Conceptual Model: Balancing Wearables in the Workplace

Based on existing literature and the chapter 2.1 the key concepts and effects presented in the conceptual model will be explained shortly.

As explained in chapter 2.1.1, wearable technology is referred to as computing devices that are attached to a human body and collect personal health data about the user (Ching and Singh 2016). Wearables worn in a work environment are for example smartwatches, headsets, or smart glasses.

A positive outcome of implementing wearables in the workplace is improved performance. (Mettler and Wulf 2019; Stein et al. 2019; Maltseva 2020; Miele and Tirabeni 2020). These wearables are worn during work, collecting reliable data on an

employee's physical activity and health status. The ongoing monitoring of these factors influences the employee's performance, thus impacting the overall success of the organisation. Working with an IoT device such as a smartwatch or a specific application, the data can be analysed with an AI tool to guide the employee. An example is provided by smart glasses which display 3D images to assist the employee to work more accurately. This technology can enhance efficiency, while simultaneously providing transparency of employee performance to employers and supervisors in order to adjust the work environment and increase productivity and motivation (Miele and Tirabeni 2020; Khakurel et al. 2017).

The constant data collection and analysis, storage and transmission from personal data to improve performance leads to a growing risk of privacy violations (Safavi and Shukur 2014; Ching and Singh 2016). Privacy risks emerge due to a range of factors, including the collection of personal data, the potential for third parties to access this data without the user's permission, and the sharing of data with external entities.

Consequently, the positive impact of the introduction of wearables in the workplace on employee performance may lead to increasing privacy concerns. Therefore, it is crucial to mitigate these risks, as privacy concerns negate the positive impact on employee performance (Safavi and Shukur 2014; Motti and Caine 2015; Ching and Singh 2016; Jacobs et al. 2019).

Employee monitoring with wearable technology can have a positive impact on employee well-being and workplace safety. This involves the employee's health and well-being at work. It involves monitoring stress levels, sedentary behaviour, and physical activity such as step count. By creating a safer and more secure environment, it potentially reduces stress and tension, thereby positively impacting well-being and motivation (Khakurel et al. 2017). Through constant monitoring, wearables collect and analyse health data and can intervene in dangerous situations to protect employees' health. For example, they can warn when lifting is too heavy or alert employees to high stress levels, allowing them to adjust their physical work or break times as outlined in chapter 2.1.1.

However, the monitoring activity may increase human rights concerns and lowers perceived employee's autonomy. For instance, changing processes based on wearables and their IoT systems recommendation may restrict employees' freedom in terms of structuring and organizing their work (Mettler und Wulf 2019).

The legal framework is essential to ensure the protection of employees' human rights and particularly right to privacy. Privacy is a human right that plays a key role in the introduction of wearable technology in the workplace, as discussed in chapter 2.1.2. The right to privacy is particularly relevant in the context of wearable technologies, which is why it will be analysed separately from the other human rights. Yet, the implications on all other human rights are from same importance. Protecting the employees' rights is important for several reasons. One aspect is, that if the business follows all legal regulations to safeguard employees' rights, it protects the business from legal consequences and potential lawsuits. Another aspect is that the invasion of their rights, even the feeling of being invaded, diminishes the positive impact of wearable technology.

Introducing wearable technology within the workplace engages multiple stakeholders at specific points. Understanding their different interests and potential involvements is important in gaining a comprehensive understanding and identifying gaps in the current framework around Wearables. To enable successful implementation, it is essential to understand and consider the interests of stakeholders from different disciplines and their potential impact on privacy and human rights.

The stakeholders' landscape is made up of entities like tech companies, organisations, government, intergovernmental organisations, and academic research (Latonero 2018).

Tech companies are shaping and developing the wearables and AI technology sector with the technological development and products and by implementing designs protecting privacy from the beginning on, having a huge impact on the AI landscape (Philip Jansen et al. 2019). Their commitment to ethical concerns about human rights and their consideration in the wearable technology development is necessary and can reduce privacy risks and human rights violations (Segura Anaya et al. 2018). Aligning the tech companies in ethics and morals, could influence the whole industry to operationalize human rights due diligence for wearables (Wagner 2016).

In addition to tech companies, the organisations using wearables possess the power to choose more secure wearable solutions, consequently impacting on the technological advancements of these tech firms. Their motivation lies in implementing such technology to increase productivity, reduce costs and optimise processes (Philip Jansen et al. 2019).

The government has the crucial role in setting the regulatory basis for wearables and AI technology and focusing on the impact on human rights and hence, including it into legislation. The interest of governments is to create a legal framework in which the rights of all stakeholders are protected. The legislation is a requirement for companies to integrate AI into national strategies and policies, and to follow a due diligence approach to human rights.

Intergovernmental organisations (IGO) are created to enable nations to work together more successfully on specific economic and social issues (Harvard Law School 2022). Examples for important IGOs in the field of human rights are the international labour organisation, the UN Human Rights Council, and the Council of Europe. They can influence and consult companies and governments on a national level regarding the protection of human rights (Latonero 2018). Even though they don't produce binding law it can demonstrate human rights violations from Artificial Intelligence and potential solutions or advice for companies how follow a due diligence approach and therefore reinforce regulations (Latonero 2018).

Academic research initiate solutions with academic evidence and help to better understand the impact and possible solutions for the convergence of wearables and human rights (Wagner 2016). Academic organisations bridge human rights, social science, technology and other disciplines to explore the full economic, legal and social implications of AI (Latonero 2018).

Work Councils, the representation of employees within a company, are crucial to secure and protect employees interests and rights (European Comission). They have the power to verify compliance with data protection and human rights laws. Consequently, they have the power to advocate for the introduction of measures to protect employees' data, privacy, and human rights, and to require the employer to do so if the existing framework is found to be inadequate. In addition, they play a crucial role in ensuring, that the interests from the employees are not overlooked (European Comission).

To conclude, companies are using wearable technology to improve performance. The continuous collection and analysis of employee data for the purpose of improving performance raises legitimate privacy concerns.

Wearables, which are also used to continuously monitor employees in the workplace, help companies to optimise processes to increase efficiency and enhance workplace safety and employee well-being. However, this practice raises concerns about

reducing perceived individual freedom and autonomy and hence, potentially violate human rights. Given the significant impact of technology in the workplace, which can bring benefits to both the company and employees as explained in chapter 2.2, it is essential to address the associated risks to employees' rights. Legislative measures and a robust legal framework are essential to regulate and mitigate these risks. Thus, it raises the question if the current legal framework is sufficiently protecting employees' rights such as the human rights and the right to privacy.

2.4 Legal Analysis: Method and Scope

During the research, it was identified that a lot of literature presents the opportunities and risks of wearables in the workplace in terms of individual and organisational aspects (Eager et al. 2020; Maltseva 2020; Miele and Tirabeni 2020; Patel et al. 2022). Extensive research was also conducted to examine technological issues of AI and wearables in relation to privacy and security (Safavi and Shukur 2014; Motti and Caine 2015; Ching and Singh 2016; Mills et al. 2016; Psychoula et al. 2020; Maltseva 2020). Some addressed legal issues, such as the impact of AI technology on human rights, and social issues, such as ethical concerns, but few studies consider all aspects and provide a comprehensive framework including legal, ethical and technical aspects in which particularly the wearable is the object of research (Motti and Caine 2015; Raso et al. 2018; Segura Anaya et al. 2018; Stefano and Wouters 2022). The conceptual model illustrates the complexity of technology introduction in the workplace by highlighting the balancing act and thus, raising the need to a more comprehensive approach to protect the employee and its rights in the workplace.
Therefore, the aim of this study is to conduct a comprehensive examination of the legal framework for wearables in the workplace, with a particular focus on privacy and human rights, in an attempt to close the research gap.

Scholars share the opinion that technology evolves more rapid and in a higher pace than the law and its regulations (Security, Privacy, and Trust in Modern Data Management 2007; Brey 2007). The legislation aims to minimise negative impact of technology in the workplace and ensure successful incorporation into the workplace without interfering employees' rights particularly regarding privacy and human rights. Therefore, the following study provides an analysis of the legal framework in the European Union for the protection of privacy and human rights in the context of wearables and to examine whether the current legal framework is robust to protect employees' rights as

illustrated in the conceptual model. Several Directives and Regulations exist to protect employees' privacy and data, particularly in the context of wearables and AI applications.

Therefore, this study aims to answer the following research questions:

- How to balance the opportunities and risks when implementing wearables in the workplace?
- Does the instruments in the European legal framework cover all potential risks arising from wearables in the workplace especially privacy and human rights violations?
- Are the current European regulations appropriate and sufficient to ensure employees privacy in times of rapidly evolving technology?
- To what extent does Germany safeguard the data protection rights of employees, and has it effectively incorporated EU regulations and directives into its national legal framework? Can Germany be considered a role model in this regard?
- How to foster a successful incorporation of wearables in the workplace?

To answer the research questions, the study focuses on the legislation in the European Union as it has one of the toughest legislations around privacy and security in the world (European Comission). The EU strived to ensure the protection of the fundamental human right to privacy when implementing such legal framework around data protection and data security. The regulatory field in the EU acts as a role model for other countries and governments (European Comission). The extent of Europe's commitment to legal and human rights concern is illustrated by various European policy documents and institutions with key importance to the Charter of Fundamental Rights which includes the European Convention of Human Rights (ECHR 2023). The Charter not only incorporates the European Charter of Human Rights, but also extends its scope to rights like the right to data protection. It improves the protection of fundamental rights by making them clearer and more understandable for citizens. In the European context, the ECHR is one of the most important treaties for upholding and protecting human rights. Specifically, in the field of artificial intelligence, the EU has introduced a European approach to promote the ethical integration of AI into the workplace (European AI Strategy 2023). The European Union is actively promoting a legal framework for AI that focuses on liability and ethical aspects. This commitment is exemplified

by the establishment of the AIDA Committee on "Artificial Intelligence in the Digital Age" and underlines the EU's commitment to this topic (AIDA Mandate 2022).

However, with the emergence of innovative technologies such as wearables and AI, the question is whether European law adequately protects employees' privacy.

In terms of European legislation, the following regulations and proposals for regulations are relevant in the context of wearable technology. The extensive explanations will be presented in the chapter overview see 3.1.1 and 3.2.1:

1. General Data Protection Regulation: This comprehensive and general EU regulation applies to all data processing activities, including those involving AI.
2. Artificial Intelligence Act (Proposal): The proposed Artificial Intelligence Act (AI Act) aims to regulate AI systems' impact on individuals' rights, including those of employees. It introduces requirements for transparency, accountability, and the assessment of high-risk AI systems.
3. ePrivacy Regulation (Proposal): While primarily focused on electronic communications, it also has implications for employee data privacy when AI systems interact with other devices for example in an IoT environment. The Regulation will replace already existing Directive.
4. Artificial Intelligence Liability Directive (Proposal): The Artificial Intelligence Liability Directive (AI Liability Directive) is a proposed regulation aimed at addressing liability issues related to artificial intelligence systems in the EU.
5. New Product Liability Directive (Proposal): The proposal for a directive proposes a number of additional requirements with regard to product liability.
6. European Labour Law: European labour law is a set of laws and regulations covering a wide range of areas related to employment, such as working time, contracts, and discrimination. One example of this is the Working Time Directive, which forms part of European labour law and regulates working time. Its aim is to protect employees' health and well-being by setting limits on working hours and ensuring they receive sufficient breaks.
7. European Convention on Human Rights: The treaty protects the fundamental human rights and freedoms in Europe. It covers a wide range of rights, including the right to privacy, right to work, and the right to a fair trial.
8. EU Charter of Fundamental Rights: The Charter is a legally binding document that outlines fundamental rights and freedoms protected within the European

Union. It covers a broader spectrum of rights than the ECHR including data protection.

These regulations establish a framework to ensure that AI applications and wearables used in the processing of employee data comply with the principles of transparency, fairness, accountability, and privacy to ensure compliance and ethical use of such technologies (European AI Strategy 2023).

For the analysis, the regulations and instruments covering data protection and human rights in European Law were examined and analysed for their possible interconnections and complementarity.

The process of identifying dominant concerns is based on an independent assessment of the legal landscape, supported by insights from the relevant literature on the subject. The research process was guided by specific keywords, notably "Wearables," "Privacy," and "Human Rights," to locate relevant papers. In the following, the study will provide answers to the proposed research questions.

3 European Legal Framework

The analysis focuses on a comprehensive examination of the European legal framework to determine its effectiveness in addressing the data protection and privacy challenges posed by wearables and IoT devices in the workplace. The primary focus will be on examining the General Data Protection Regulation, which is the key regulation concerning data privacy. Additionally, other current regulations such as the AI Act and the ePrivacy Regulation, which aim to protect individual privacy, will also be examined, and set into context with the GDPR. A further area of focus for this study will be the exploration of the human rights implications of integrating wearables into the workplace (see chapter 3.2).

3.1 European Legal Framework for Privacy

The European Legal Framework regarding Privacy will be presented. A brief overview and definitions of the main terms introduced in the legislation set the basis for the analysis of the legal framework to protect employee’s privacy.

3.1.1 Overview

The relevant regulations and directives in the European legal framework regarding privacy and data protection for wearable technology are the General Data Protection Regulation, the proposed Artificial Intelligence Act, the ePrivacy Regulation and the Artificial Intelligence Liability Directive and the New Product Liability Directive (European Parliament; Council of the European Union; European Parliament 2023; European Digital Strategy 2023; European Comission 2021).

European Legal Framework	Effective Date
Privacy	
General Data Protection Regulation	25 of May in 2018
Artificial Intelligence Act	expected end of 2023 European Comission
ePrivacy Regulation	expected end of 2023 European Comission
Artificial Intelligence Liability Directive	expected 2024/2025 European Comission
New Product Liability Directive	expected 2024 European Comission

Table 2 Overview of the European Legal Framework around Privacy

The General Data Protection Regulation, short GDPR, is a European law put into effect on May 25, 2018, that aims to protect data of individuals and give them the control over whole data processing cycle of their personal data to ensure their privacy (European Parliament; Council of the European Union). It is the most important regulation ruling data protection (European Parliament; Council of the European Union). The GDPR was created to enshrined on the fundamental right to the protection of personal data, set out in the EU Charter of Fundamental Rights (European Comission). Several updates and extensions leading to the current version of the GDPR EU 2016/679 including ninety-nine articles and 173 recitals. The challenge of data protection is not a new topic covered by EU legislation. With the fast progress of emerging technologies and the internet, the EU needed to update the existing data protection directive to ensure it is sufficient to protect data and covers the new risks imposed by the technological progress (European Comission).

The GDPR applies for companies processing data from EU citizen or residents. Further, the data must not even be exported from the EU. The servers containing personal information need to be located in the EU. Important here is to mention that it is

regardless of the location of the company. It can apply for companies even outside of the EU under certain conditions (GDPR, Article 3). If companies are trading with companies in the EU and therefore offering products to EU Citizen or monitor their online activities (European Comission). For example, a company based in Asia still need to comply with the GDPR if it sells products to EU companies and therefore the EU market targeting EU citizens. There are two exceptions in which the companies or individuals are fully or partially free from falling into the legal scope of the regulation. First, if the data collected is purely for “personal or household activity”. The regulation just applies for companies acting in a “professional or commercial” way (European Comission). Second, it just partially applies for companies fewer than 250 employees.

For companies which need to comply with the regulation, the regulation poses great responsibilities and obligations in terms of data protection and privacy, and heavy fines for non-compliance. Companies that do not comply with the regulation face a fine of up to 4% of their annual revenue or €20 million (European Comission). It depends on the type of violation and the company's financial resources (Wolford 2020). For example, inferences against the basis of the Regulation like the right to privacy and right to be forgotten will be charged higher (Wolford 2020). It is ensured that companies not complying are subject to significant liability. Deciding and administrating about fines is responsibility of the data protection regulator of each EU country (Wolford 2020).

The General Data Protection Regulation is an independent legislation addressing risks and vulnerabilities in terms of data protection in a digital environment in general. It does not specifically address AI technology or wearable technology (Mitrou 2018). Thus, it is crucial to analyse the regulation regarding specific emerging technology such as wearable technology and AI to ensure it is applicable to it.

Aside from the general data protection regulation, the Artificial Intelligence Act is a proposal from the European commission to regulate artificial intelligence (European Parliament 2023). It was first presented in April 2021, aiming to complement current European legal framework in addressing risks related to AI to make AI system more trust-worthy to promote development and adoption from AI technology, including wearables. Thus, it is narrower compared to the GDPR which aims to regulate privacy and data protection especially in a work environment (Stefano and Wouters 2022). The AI Act got approved in the European parliament on June 14, 2023, and will be discussed and negotiated from the EU states. It is planned to have a final draft end of the year 2023 (European AI Strategy 2023). It addresses potential risks arising from AI by

classifying different AI systems according to their inherent risk (European Parliament 2023). Wearable devices equipped with AI capabilities can be classified as minimal, limited, or high risk depending on the context in which the wearable is used and the type of wearable. Limited risk means that wearables allow the user to make informed decisions and are aware of the interaction with an AI tool. Wearables equipped with AI capabilities or connected IoT devices have the potential to make automated decisions, but the ultimate decision to accept or ignore those decisions remains in the hands of the user (Stefano and Wouters 2022).

For instance, in a logistics warehouse, augmented reality glasses are anticipated to propose the shortest route which users are likely to follow. Inaccurate data or occasional routing errors, while not ideal for optimal performance, usually do not significantly impact the safety of employees. However, if the wearable technology or connected IoT device is capable of making automated decisions that could have serious consequences for human safety, then it may be classified as a high-risk device. For AI systems with limited or minimal risk, not as many legal obligations are required because their potential impact on human health and safety is limited and therefore only transparency requirements are needed. High-risk systems are subject to strict requirements to ensure that they do not negatively impact privacy and human rights. These include rules on testing, documentation of data quality and, most importantly, accountability, which complement the GDPR and potentially close security gaps (European Parliament 2023).

The ePrivacy Regulation, also known as the ePrivacy Directive, is a European Union regulation to protect privacy in electronic communications. It covers aspects such as confidentiality, consent to data processing and rules on electronic marketing and cookies. The regulation aims to protect citizens' personal data and online privacy and to ensure that their electronic communications remain confidential and secure. It complements the GDPR by addressing specific data protection issues related to electronic communications including machine-to-machine communication.

The AI Liability Directive is a proposed regulation that addresses liability issues related to artificial intelligence systems in the European Union. It aims to establish a legal framework for determining liability when AI systems cause damage or harm. This directive aims to provide clarity on who should be held responsible in cases of AI-related incidents (European Comission 2021).

In the next chapter the main legal aspects of the European legal framework governing wearable technology will be analysed to understand its instruments and limitations to protect privacy. The principles of the General Data Protection Regulation form the basis of the analysis and are complemented by the proposed AI Act, the ePrivacy Regulation and the AI Liability Directive to show all the instruments used or about to be used in the legislation to regulate such technologies and make assumptions about potential risk vulnerabilities to privacy of the employee.

Particularly relevant for wearable technology are the legal ground and informed consent, the data protection principles and privacy by design and default which will be the object of analysis.

3.1.2 Terminology

Before going into the depth analysis of the instruments in the EU Law, the main legal terms introduced in the Regulations will be explained first. Further, the study explores the principles forming the basis of the regulation aiming to protect employee data and privacy and analyses their effectiveness in the context of wearables.

The regulations govern the protection of data especially personal data. The GDPR defines personal data as “any information relating to an identified or identifiable natural person; identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (Stefano and Wouters 2022). Therefore, biometric data, health data and location data all belong to personal data. The definition offers room for interpretation regarding the identifiability of the person (Mitrou 2018). It is crucial to understand the concept of identifiability because it leads to the applicability of the law (Mitrou 2018). The GDPR does not apply for anonymous data and therefore information that is not identifiable but even from anonymous data conclusions can be drawn to a person and if this is relatively easy, it falls under the scope of the GDPR (European Comission). If the data is clearly identifiable to a person, the regulation is applicable, regardless of the intentions (Mitrou 2018).

Data processing refers to the “set of operations carried out on personal data” (Wolford 2020). This involves for example the collection, transmission, analysis, and storage of the data.

The personal data collected and processed belongs to the data subject. The GDPR aims to ensure the control of the data subject about their data (European Comission). Data subjects have the right to object to processing (Rodrigues 2020).

Another important term is the data controller defined as the person or company, collecting, and processing the data from the data subject (European Comission). The decisions made about the utilisation of the data are made from the data controller after ensuring to have the approval of the data subject to process the data (European Comission).

In case that the data controller decides to involve a third-party to support the data processing for example a cloud service, this party is defined as the data processor (European Comission). For the data processor specific rules apply.

In the scope of this study, the data subjects are the employees, and the data controller is the company implementing wearable technology in the workplace. Wearables are collecting health data which is falling into the scope of personal data which is the first argument why the GDPR must apply to wearable technology. Therefore, processing the personal data requires several regulations to protect the fundamental rights (Stefano and Wouters 2022). A data processor may be involved for storage of the data in the cloud or data analysis tools offered and operated by third party providers.

Despite the GDPR's attempt to accurately define legal terms, gaps remain that allows for interpretation, potentially resulting in legal uncertainty (Mitrou 2018). The regulation applies universally to companies across all industries, types, and technologies involved in data processing, creating room for varying interpretations.

After clarifying the terms, the following analysis examines the key instruments introduced in Europeans legislation to protect employee privacy.

3.1.3 Analysis

The International Privacy Principles established and formulated by the Organisation for Economic Cooperation and Development are playing a key role in shaping the evolution of privacy regulations (Brey 2007). The following key privacy principles are the main instruments on which the GDPR is based to ensure data protection and privacy (GDPR, Article 5).

To begin with, the GDPR outlines two requirements that must be met to legitimately process personal data.

First, to be allowed to process data a valid legal ground needs to be found (GDPR, Article 6). The following legal grounds could be relevant in the context of wearable technology.

A legal ground could be the need for a contract with data subject participation, for example, if the data subject is a party to a contract (GDPR, Article 6). For instance, the data needs to be collected to make sure that the employee has the health requirements for the job. Here it is crucial to define the necessity which offers space for interpretation. It can be defined as necessary if it is needed to keep the business running (Stefano and Wouters 2022).

Another legal ground validating the data processing is the “public or legitimate interest” (GDPR, Article 6.1). The data is necessary to perform a task for the public or the data controller has a legitimate interest to process the data. Here it is clear that it is a matter of interpretation and explanation if the lawful basis accounts or not. It is the legal ground with the highest scope of interpretation possibilities since it is not clearly defined what legitimate interest involves. However, most importantly the interests must be evenly distributed for the two parties considering the advantages and disadvantages for the data controller and data subject to be considered as a legal ground.

Lastly, an applicable legal ground involves acquiring “informed consent” (European Comission). However, when it comes to employers aiming to introduce AI technology, relying solely on employees' consent for data processing typically doesn't qualify as a valid legal ground (Stefano and Wouters 2022).

Therefore, for the case of introducing wearable technology in the workplace, the legal ground of “legitimate interest” may apply. It could be argued that the monitoring of performance is in the interest of the company to enhance organisational performance, but as well increasing employee well-being and performance as outlined in chapter 2.2.2. Data collection for pure performance tracking could be considered legitimate. Analysing the data to improve performance by for instance establishing more efficient break times could also be considered legitimate. However, using the data to draw conclusions that the employee is unable to meet a certain standard of performance could be considered an intrusion in privacy and employment rights.

Nevertheless, it can be argued that the right to privacy of the employee may be invaded if the company collects the health data to take advantage of it or resign the

employee based on that. This could also restrict the right to freedom and right to employment and by that entering the area of human rights.

The argumentation shows the challenge to find a legal ground for processing personal data collected by wearable technology in the workplace. The legal ground must be communicated for transparency with the data subject (GDPR, Article 4).

Finding a legal ground for data processing is the first requirement to be allowed to incorporate wearable technology. In addition to the legal ground, a permission is required to process data the so-called informed consent of the data subject (Segura Anaya et al. 2018). It is covered by several articles, which highlights the importance of it (GDPR, Article 4, 6 and 7). The consent is bound by rules. It must be “freely given, specific, informed and unambiguous”, to ensure that no misunderstanding or language barriers misleading the data subject to give a consent (Wolford 2020). It is highlighted that the language must be “clear and plain” to avoid grey areas and the exploitation of the consent. In any case the data subject can remove its consent at any time without the need to give explanations or fearing consequences (Wolford 2020). If a legal ground can be identified and the processing is approved by the data subject with an informed consent, the GDPR comes into effect.

In the following, the study explores the key privacy principles forming the General Data Protection Regulation and analyses their effectiveness in the context of wearables. It will be elaborated how other Regulations regarding privacy are complementing the GDPR such as the AI Act, the ePrivacy Regulation and the AI Liability Directive.

The six following principles relating to processing of personal data are set out in Article 5 of the GDPR.

General Data Protection Regulation Principles			
1	Lawfullness, Fairness and Transparency	4	Data Quality
2	Purpose Specification	5	Data Security and Confidentiality
3	Proportionality	6	Accountability and Liability

Figure 3-1 General Data Protection Regulation Principles

Lawfulness, fairness, and transparency

The GDPR defines that the data processing must be lawful, fair, and transparent in relation to the data subject (GDPR, Article 5.1a). The processing is lawful when a legal ground can be found (GDPR, Article 6). As explained before, the legal ground for introducing wearables could be the legitimate interest of the company to justify the data processing.

Fair processing aims to balance the interests of the controller and the data subject. (Şandru 2020).That means balancing the interests of the company with employees' personal rights. Fairness does not only include the verifiable fact of being fair in terms of being lawful, but it goes beyond this aspect. It is related to the provision of information about data collection and processing and that all information necessary for the data subject are provided and communicated (GDPR, Article 2 and 14). Therefore, fairness represents both lawful behaviour and a value system characterized by impartiality and appropriateness.

While fairness is closely related to transparency, it goes beyond transparent communication and also includes appropriate behaviour towards the data subject (Mitrou 2018). Defining the principle of fairness is complicated because it depends on subjective factors such as what kind of behaviour is considered fair (Şandru 2020). But it can be said that the concept of fairness does not primarily relate to the rights of data subjects, but rather to the behaviour of data controllers towards them and consequently, the respecting treatment of the employee rights (Mitrou 2018). The company needs to ask itself if the collection of data is necessary and if the analysis of it is fair and as well the consequences deriving out of it.

Data processing must also be carried out transparently (GDPR, Article 5.1a). That means the company needs to be transparent to the employee about the whole data processing cycle. That includes the data collection, which data will be collected, processed and in which way will it be processed, on which legal ground will the data be processed and importantly what is the purpose of the data collection. Additionally, transparent communication regarding the wearable technology utilized for data collection and analysis, as well as the storage location of the data, is integral to maintaining a transparent approach for personal data processing.

Since the principle is so fundamental for data processing it is crucial to check if the legal ground is valid and if the degree of fairness and transparency that companies introducing wearable technology can offer is sufficient to comply with the GDPR. As mentioned before, to lawfully incorporate wearable technology and validate the data processing of employee data, the legal ground of “legitimate interest” may apply. Enhancing organisational performance and considering the beneficial effects for employees, like increased well-being and workplace safety, could classify as valid reasons to be allowed to process data.

However, the adoption of wearables and the associated risks and opportunities must balance the company's interests in increasing performance. When wearables are utilized to improve workplace safety and the well-being of employees, it can positively impact business performance by increasing employee engagement and reducing turnover or sick days, and increasing productivity (Miele and Tirabeni 2020).

Nevertheless, companies should be aware of the potential impact on mental health and the possible negative consequences of monitoring. It is important to ensure that monitoring is balanced and does not overshadow the company's commitment to the interests and rights of employees. The company may conduct regular evaluations and meetings to ensure that the technology's impact aligns with both the company's interests and the rights of employees. By doing that it can be argued that the company is acting lawfully fair and in awareness of the employees right, which leads to compliance with the principle.

Further, the GDPR also requires transparency in data processing (GDPR, Article 5.1a). The GDPR does not clearly define the scope of transparency. Neither does it consider if it is possible in context of innovative technologies to reach such high degrees of transparency that would be necessary for the employee to fully comprehend the data processing. The challenge with wearable technology especially AI wearables arises if it is possible to be as transparent as it would be necessary for the data subject to be able to understand the steps and underlying analysis in the data processing to give a consent. For instance, transparency about the purpose and nature of the data collected is achievable, but full transparency, including explanations of the underlying technological processes in wearables and IoT devices and especially AI wearables for data analysis, presents difficulties.

Here the proposed AI Act may complement the GDPR. It points out the necessity of checking AI tools carefully for biases to avoid unfair decisions which the AI tool is proposing. It obligates the provider of the system to examine the data collection and

analysis on biases and suitability. The proposal emphasizes like the GDPR the clear transparency about the data use (European Parliament 2023). The AI Act aims to define the necessary degree of transparency required for data subjects to provide informed consent for the processing of their personal data (European AI Strategy 2023). It addresses the lack of definition of transparency in the GDPR. Yet, it remains difficult to understand underlying technical processes for the data controller and therefore for the data subject, to understand how and why the AI system took a specific decision. Even though this lies in the nature of an AI system it can be considered critical in terms of ensuring employee data protection when wearables are introduced in the workplace.

Purpose Specification

To meet requirements of transparency the purpose of data processing must be clearly defined and communicated to all parties. This leads to the next principle of purpose limitation (GDPR, Article 5.1b). The data must be “collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes” (GDPR, Article 5.1b). The paragraph states that the purpose must be well-defined and transparent to the data subject from the beginning on. This allows the data subject to give informed consent while ensuring that the transition from raw data to processed data is necessary for the purpose and only serves the purpose. In this context, it is essential to ensure that any analysis conducted does not change the original purpose or legal ground. The purpose limitation principle is a fundamental principle also included in the Charter of Fundamental Rights (Mitrou 2018).

The purpose of using wearable technology in the workplace could be to improve performance. However, this purpose of improving performance requires a clear and precise definition. It is therefore a matter of specifying what performance is, how it is specifically measured, and what data is associated with it to comply with the principle. The health data collected from employees must be exclusively to achieve this purpose, so the collection is limited to these essential data.

If the wearable technology also makes it possible to recognise health issues of employees, it serves a different purpose than originally intended. This deviation could potentially lead to prohibited actions on the part of the company. As a result, even if the purpose is not to reveal such issues, the company must be careful to ensure that the processing of data does not unintentionally draw conclusions about the employee's health. For instance, considering a scenario in which an employee wears a wearable

such as a smartwatch intending to enhance efficiency. These wearables often have a built-in GPS system that continuously records the employee's location as soon as the wearable is worn and, in many cases, cannot be switched off. This could unintentionally give the company insight into the employee's behaviour and not just support them perform their work. While these insights do not violate policy, they could provide the company with insights that are not desired and accepted with the given consent from the employee, which could compromise the employee's privacy rights.

Proportionality

The so-called “Data Minimisation Principle” is the principle of collecting and processing only as much data as necessary for the specific purpose to keep it proportionate (GDPR, Article 5.1c). This involves considering the quantity of data collected and the extent to which it is processed. In other words, collect as little data as possible and process it as little as possible (European Comission). This principle aligns with the “purpose limitation principle”, emphasizing the necessity to remain within the defined scope of purpose and collect data solely for that specific purpose. This concurs the fact that the whole data processing and collection practice must be proportional to the purpose that means only the data required is allowed to be collected and processed (European Data Protection Supervisor 2023).

The "storage limitation" principle is aligned with the principle of proportionality and states that data should not be kept longer for the original purpose upon it was gathered (GDPR, Article 5.1e). Exceptions are made for scientific or historical research, always with the consideration for safeguarding the rights and freedoms of the data subjects. The principle ensures compliance with the data subjects' privacy right, specifically the right to be forgotten (GDPR, Article 17). The question of proportionality is crucial here, because it is relevant to the limitation intentions of data collection, processing, and storage.

In the case of wearable technology, it is important for the company to carefully consider the scope of data the wearable device is collecting to follow the principle of data minimisation and purpose limitation and to make sure the data collecting is obligatory to achieve the purpose. For example, using a wristband attached to a helmet that measures fatigue and alertness can monitor data about brain waves, heart rate and temperature. Because the wearable continuously tracks the employee's data throughout its use, it collects a significant amount of information. The company must ensure,

that all data is relevant to achieve the purpose of increasing employee safety in the workplace. The analysis of the data must be limited exclusively to fulfil this security-related purpose, ensuring compliance with GDPR, and preventing any invasion of privacy. For instance, if the ability to measure the temperature is not relevant to detect fatigue and alertness or the workplace does not expose to relevant temperature changes, the wearable should not collect this data set. There must be the possibility to turn of unnecessary features or simply develop wearables with explicit purpose for the company to minimize data collection. If this is not feasible for cost and effort reasons, it remains unclear whether wearables therefore fully comply with the principle of proportionality and as well purpose limitation to protect employee data always and in every context.

In addition, the company must assure that the storage of data is deleted regularly and checked if the stored data is still necessary to serve the purpose to comply to the storage limitation principle. It must constantly question whether the storage of the data is relevant and how long the data should be stored to comply with the principle.

Data Quality

The data quality is crucial to avoid misleading information and predictions from collected data for example regarding performance at work or employee's health situation. Data quality relies on the precision of the data and on keeping the data up to date whenever possible (GDPR, Article 5.1d). The General Data Protection Regulation states that quality includes not only the quality of the personal data itself, but also the accuracy and quality of the analysis, processing, and deletion of the data. In addition, the data must be relevant to the purpose of the processing which aligns with the purpose limitation principle and proportionality (GDPR, Article 5.1d).

The principle poses a challenge for data protection and privacy rights of employees when companies are introducing wearables, because the data they collect and record may not always be accurate and thus, leading to incorrect analysis and inferences (Stefano and Wouters 2022). Not complying with the principle provides an opportunity for the data subject to oppose to the processing and collection of the data (Stefano and Wouters 2022). This would cancel out the positive effects of introducing wearable technology into the workplace for the company or even deny the company the legal ground for data processing.

Regarding the completeness and accuracy of the data, the company must trust in the wearable technology and the tech company developing it that the design, and installed sensors are of latest standards to guarantee accurate data collection. Collaboration with the developer is possible to ensure that the technology meets the latest standards. This also requires technological knowledge within the company to ensure data quality, compliance and to be able to control the developer. Further, the company must ensure to update the software and data regularly. The data quality can also be defined in a Code of Conduct as a best practice.

Data security and confidentiality

According to the principle of "integrity and confidentiality" the personal data needs to be secured appropriate to ensure confidentiality of the data (GDPR, Article 5.1f). This demands protection against unauthorised access and processing by third parties, potential loss, damage, or destruction. Both technological measures and organisational processes must be implemented to ensure the data security. The technological and organisational measures that could be taken to secure the data should be appropriate and are defined in the GDPR like following. For technological measure, the GDPR points out for example the two-factor authentication and encryption of data for data transmission. Organisational measure means offering staff training, limit data access and implement a code of conduct (Wolford 2020).

Moreover, the principle of integrity and confidentiality encompasses the data subject's privacy rights namely the right of access and free flow of data (Brey 2007). The person is allowed to access their data and to keep them in a more appropriate form and to share them himself if desired without any interference from the data controller (GDPR, Article 15 and 20).

The ePrivacy Regulation complements the GDPR in terms of confidentiality. It complements the GDPR in aiming to ensure specifically confidentiality of electronic communication data including the machine-to-machine communications and thus IoT (European Digital Strategy 2023). Any inferences if not permitted by the ePrivacy Regulation are prohibited. For instance, the data security during data transmission and consequently the communication between wearable and IoT device is regulated and protected by the ePrivacy Regulation. It is aligned with the Article 7 of the European Charter of the Human Rights in terms of respecting the person's private life (European Digital Strategy 2023). The privacy of the user is object to the regulations and must be protected through the whole communication process.

The regulation states that data transmitted from one device to another must be anonymized and meaning deidentified (GDPR, Article 5; ePrivacy Regulation). It clearly regulates that machine-to-machine communication need to ensure confidential communication to protect the data transmitted.

The company must secure access to the wearable, the IoT device and the storage with, for example, two-factor authentication as suggested in the GDPR to limit the data access and ensure confidentiality of the data. Further, the company should ensure that the wearable technology and the connected IoT system implemented, can deidentify collected data so that the protection of the personal identity of employees can be maintained even in the event of unintentional loss or access to the data. An insecure connection over which the data is transmitted also poses a risk of violating the principle of confidentiality, as unauthorised access may occur. However, in the case of deidentified data, the consequences are less severe, as they cannot be exploited to manipulate specific individuals and therefore as well result in lower fines for the company. This is another reason data should be encrypted and therefore deidentified from the beginning on, so that any unintentional interference in the data process is less severe. It is therefore the company's responsibility to ensure the use of secure wearable technologies and connections, such as secured Wi-Fi and Bluetooth, to prevent access by third parties to follow legal requirements. These measures ensure legally compliant integration of the technology into the work environment and the protection of employees' rights regarding privacy and personal data protection.

Accountability and Liability

The principle of accountability means that the data controller must demonstrate that he complies with the provisions of the GDPR. This means that he must be able to demonstrate the type of data collected, the intended purpose and the way they are processed (GDPR, Article 5.2). Accountability essentially puts the responsibility on the data controller, which may subsequently lead to potential legal obligations and liability. In case of neglectful liability, the data controller must compensate the data subject in case of damages to said subject or unlawful data processing which scrutinises the data of the data subject

When AI systems are used in the workplace, the data subject has the right to challenge the decisions proposed by an AI system and to request a review of the data

collected. In situations involving damages or discriminatory behaviour, the question of liability then comes up (Kingston 2016).

Further challenges related to wearables may arise when attempting to clarify the processing of personal data involving AI and automated decision (i.e., Google Glasses). In particular, systems driven by artificial intelligence that make decisions without explainable reasons, for instance if there is an algorithm behind, raise fundamental accountability concerns (International Conference of Data Protection 2018). This means that the decisions AI makes must be reviewed, explained, and evidenced to ensure that they are unbiased and free of discriminatory actions, and to meet accountability. However, it is often not possible to understand why an algorithm decides the way it does (Mitrou 2018).

That is why with AI in the workplace arise challenges of accountability and transparency due to the complexity of the data analysis (Rodrigues 2020). The GDPR does not provide sufficient protection against sensitive inferences or challenge decisions based on inferences (Wachter and Mittelstadt 2018).

The current liability framework for wearables includes the “Product Liability Directive 85/374/EEC” that offers a civil liability framework for ruling damages caused by products or services (DeLuca 2023). For instance, this directive applies to cases involving products like non-AI-enabled wearables and IoT systems, such as the application or mobile devices connected to the wearable. Civil liability governs the responsibilities of one party in situations where another party suffers from damages (Dictionary Cambridge). The rapid development of innovative technologies is raising concerns about the sufficiency of current liability rules. These regulations were introduced in 1985 and there is uncertainty regarding their adequacy in managing emerging risks and providing clear compensation guidelines for damages in current times of new technologies (Madiega 2023). Recognising this, the European Commission proposed an updated version in September 2022, revising on the strict liability of manufacturers, the “New Product Liability Directive”. This revised version introduces new possibilities for claims for damages and liable parties. The scope of liability is expanded to include all parties involved in the product development process who may be responsible for defects and resulting damages, except of only the manufacturer (DeLuca 2023). It is important to note that the directive solely focuses on “material” damages, such as data loss. In contrast, the GDPR covers both “material” and “immaterial” damages caused by data processing and thus including intangible violations like inferences against

human rights (DeLuca 2023). Yet, the New Product Liability Directive is not sufficient to cover all requirements exposed by the innovative technology AI.

In response to these gaps, the European Commission has put forward a proposal to strengthen accountability within the GDPR framework and establish liability rules for products or technologies that do meet AI requirements and therefore, fall outside the scope of the Product Liability Directive (PLD) (European AI Strategy 2023). This initiative, known as the AI Liability Directive, was presented alongside the AI act to complement the existing legal framework. While the AI act aims to mitigate AI-related risks, the directive focuses on defining liability and compensation claims in cases where AI-related risks lead to harm (Madiega 2023)

In the current proposal the developer of the AI systems is responsible for the consequences of using AI systems and any failure or unpredicted outcomes of it (Madiega 2023). The directive's scope cover harm caused by AI systems to both individuals and legal entities, including businesses. In contrast to the new PLD covering primarily private persons who able to claim for compensation (DeLuca 2023). The current legislation generally includes fault-based liability principles, meaning that the injured party must prove the responsibility party's fault. The new AI directive offers an alternative, permitting claims for damages in business operations that involve AI adoption without necessitating a strict fault-based approach. Under the fault-based approach, the injured person must prove that someone was at fault for the damage. Thus, it is especially important to refrain from this approach given the complexity of AI systems. The complexity makes it difficult to match specific inputs to the resulting outputs that led to the damage and thus, proving someone's fault.

For companies that use wearables in the workplace, the implementation of the proposed directive would potentially reduce their immediate liability concerns in the event of harm caused by AI-enabled wearables. Even if harm does occur, these companies could seek compensation from the manufacturer or developer, i.e., those involved in the development process of the wearable. This approach shifts liability away from users, particularly employees, who would otherwise have to prove a technology-related defect in case of damages in the workplace when wearing wearables. It further shifts liability from the company only implementing the technology to the manufacturers developing the technology in case of technological failure or damages related to incorrect

decisions made by an AI-enabled wearable. And thus, strengthening employees' rights.

In addition, the directive expands the scope of liability to include possible violations of employees' data protection and privacy rights. This includes cases of data loss or other forms of damage that violate employees' privacy. This proposal ensures that employees are covered with compensation when their privacy rights are violated. Yet, whether and to what extent the company can ultimately pass on responsibility and hold an AI system accountable remains questionable.

However, the issue of liability remains of importance in protecting employees in their work environment, especially when they are provided with technological tools to perform their task. As a result, technology is part of the output of the decision-making and task execution process and may therefore partly to blame for possible failures.

To conclude, the GDPR lays out two requirements which need to be met to be allowed to process data in the first place. If these requirements are met and personal data is processed, the GDPR applies. The regulation consists of six key instruments to ensure data protection, complemented with the concept of privacy by design and default. The proposed AI Act, AI Liability Directive and the Privacy Regulation are complementing the legal framework regarding privacy and data protection in context of wearable technology. The analysis pointed out the effectiveness of the implemented instruments in the European law and which role they are playing for safeguarding employees' privacy when implementing wearable technology in the workplace.

3.2 European Legal Framework for Human Rights

Giving a brief overview of the current legal framework for human rights will set the basis for the further analysis of the instruments introduced in the legislation to prevent violations against human rights when implementing wearable technology in the workplace.

3.2.1 Overview

The European legal framework regarding human rights includes the European Convention of Human Rights, the European Charter of Fundamental Rights, the European Labour Law and the GDPR (see Table 2).

European Legal Framework	Effective Date
Human Rights	
European Convention of Human Rights	03 of September 1953
European Charter of Fundamental Rights	December 2009
European Labour Law - Working Time Directive - Transparent and Predictable Working Conditions Directive - Termination of Employment	 - 04 of November 2003 (Update 2023) - 20 of June 2019 - 23 of November 1982
General Data Protection Regulation	25 of May in 2018
Corporate Sustainability Due Diligence Directive	expected 2026 European Comission

Table 3 Overview of the European Legal Framework around Human Rights

The preamble of the GDPR states the link to the European Union Charter of Fundamental Rights (Stefano and Wouters 2022). The GDPR aims to protect primarily the right to data protection and the right to privacy. Wearable technology in the workplace influences the privacy of the employee mainly through the processing of their personal data making the GDPR applicable. But wearables have as well significant implications for human rights since it is implemented in a workplace working with humans. Thus, the further analysis focuses on analysing the human rights implications apart of only focusing on the human right to privacy. The Fundamental Rights Charter is also considered in the analysis, since the international Declaration of Human Rights, as one of the most relevant documents for human rights, is laid down in the European politics in two documents, namely the European Convention of Human Rights and the Charter of Fundamental Rights. For example, the right to data protection is not a human right but part of the Charter of Fundamental Rights and yet relevant to assess the privacy impact of wearables.

In providing an overview of the European legal framework in relation to wearables, it is therefore important to analyse soft legal instruments such as human rights, in addition to hard legal instruments such as the GDPR, to be able to answer the research question of whether the legislation is sufficient to protect not only employees' privacy but also all their human rights.

3.2.2 Analysis

The European Convention on Human Rights will be the basis for further analysis of human rights implications. In the context of wearables and AI particularly important to

protect are the right of privacy, equality, and no discrimination (ECHR, Article 8 and 14).

The potential human rights implications are presented in the table below and will be elaborated upon in the following, along with how the legal framework protects them.

Effects of Wearables Implementation	Potential Human Rights Implications
Comparison of performance data, biased algorithm	Right to non-discrimination, right to equality
Severe changes in the job market	Right to work, right to protection against unemployment, right to favorable work condition
Blurred lines between break and work time	Right to favorable work condition
Dehumanisation of the workplace	Right to favorable work condition
Overuse of fixed-term contracts	Right to work, right to favorable work condition
Technical privacy risks	Right to privacy
Liability Issues	Right to fair trial, right to access to justice
Misleading data analysis and bad data quality, biases in data	Right to fair trial

Table 4 Human Rights Implications

The amount of data collected with wearables and further data processing, including data analysis, may lead to unequal treatment of employees. There is a possibility of discrimination based on performance data, which may lead to violations of human rights to non-discrimination at the workplace and equality as laid out in 2.2 (Rodrigues 2020).

For instance, it may lead to discrimination if the manager favours one employee based on performance data or dismisses another employee based on weaker performance, even if the latter accomplishes the required task in the given time but does not perform at the level desired by the manager. The possibility of direct comparison of performance levels can then lead to a violation of the human right to equal treatment at work and consequently, favours discriminatory behaviour. Another aspect is the lack of transparency of algorithm behind a wearable or an IoT Device, executing the data analysis may lead to biased and discriminatory outcomes of the analysis or decision proposed by the technology.

Additionally, using wearables and setting performance standards based on them can potentially violate the fundamental human rights of people with disabilities,

particularly their right to work and equal treatment (Latonero 2018). Relying heavily on wearables for performance evaluation risks overlooking the unique challenges and abilities of people with disabilities, which can lead to discriminatory practices in the workplace.

Several instruments implemented in the GDPR may protect such violations of human rights to non-discrimination and equality.
The principle of defining a specific and explicit purpose laid down in the GDPR may restricts the data analysis and the possibilities of exploiting analysis and conclusions made from the analysis to prevent discriminatory outcomes.

Another principle of the General Data Protection Regulation relevant to protect against data misuse and reduction of the probability of data being used for discriminatory purposes is the principle of data confidentiality and integrity. This is achieved by limiting access to data and devices through secure authentication systems and requiring deidentification of personal data.

Ensuring transparency with respect to data processing when using performance data is as well essential to protect the right to non-discrimination and equality and prevent potential abuse of the data (Sekalala et al. 2020). Transparent processes may ensure, that AI systems decisions or the data sets filling them are not biased and thus, taking discriminatory decisions. Especially wearables with AI capability could override the decision of employees leading to inequalities between technology and human and therefore leading to discriminatory effects, if the AI system is biased (Latonero 2018). The existing legal framework primarily focuses on preventing traditional forms of human discrimination, which differ significantly from the more subtle, intangible, and challenging-to-detect automated discrimination (Wachter et al. 2021). There is scope for strengthening the current legal framework to detect and prevent automated discriminatory activity.

Introducing innovative technologies like wearables in the workplace has significant implications for working conditions and the job market, as highlighted in the study "AI and Digital Tools in Workplace Management and Evaluation". This impact encompasses various aspects, including the creation of new job roles, changes to existing ones, alterations in remuneration, concerns related to health and safety, shifts in the job market, and potential employee dismissals (Rodrigues 2020).

The integration of wearables may lead to new work requirements being created or existing work profiles being changed, requiring staff to be retrained, a challenge that may not be feasible for everyone. As an example, wearables can collect data to fill scheduling systems powered by AI, which can optimise work schedules, ensuring that the necessary skills and the right number of employees are available precisely when needed. This can result in a reduction in the overall workforce size. These impacts have the potential of violating the human right to work and the right to protection against unemployment due to severe changes in the job market (CFR, Article 15 and 31). Protection from unemployment requires a commitment by enterprises to provide employment opportunities and access to paid work. It is important to recognise the interdependence between the right to work and protection from unemployment, as one cannot fully enjoy the right to work if one is not protected from unemployment (Hornuf et al. 2023). The International Labour Organisation (ILO) has included regulations in labour law to set standards for the termination of employment. The Convention to Termination of Employment, 1982 states for instance justifications reasons for termination and a procedure against termination. Employees cannot be dismissed based on their race, gender, or political opinion or for misconduct (International Labour Organisation 6/2/1982). However, dismissals and terminations of employment based only on poor performance are permitted and may make it more difficult for employees with poor performance. AI and wearables can quantify performance and personnel decisions can be made based on it and thus, may violate the right to protection from unemployment.

Further, the severe changes in the labour market may have implications for the right to favourable conditions of work. Favourable working conditions include elements such as fixed break times and the avoidance of overtime, as well as ensuring a safe and healthy working environment.

Wearables have the potential to blur the lines between worktime and breaktime when employees use wearables in the workplace and thus may violating the right to favourable working conditions (Stefano and Wouters 2022). Regularly and time-fixed break times are crucial to uphold this right.

The GDPR does not offer legal protection to safeguard the human right in the first place but the labour law specifically ruling the workplace introduced instruments that may protect it. The Working Time Directive (WTD) as part of the labour law outlines specific break hours relative to total working hours (European Parliament; Council of the European Union 8/2/2004). Consequently, it sets a legally mandate break times to

prevent violations against the right for favourable working conditions. Ensuring that wearables do not disrupt employees during break times, for instance, by sending alerts for physical inactivity or work-related notifications, is therefore crucial to protect and comply with the human right (Stefano and Wouters 2022).

Additionally, the right to disconnect outlined in the labour law, protects the right as well to favourable working conditions. Employees have the right to disconnect from work-related apps or take of the wearable's device outside of working hours without facing consequences from the employer (WTD, Article 9 and 10). That reduces the potential interruption in their personal sphere and improves working conditions. Compliance with this principle can be achieved through design and the default settings of wearables. As highlighted by Rodrigues (2020), default settings that are appropriate can ensure GDPR compliance (Rodrigues 2020).

Furthermore, wearable technology's potential to dehumanise the workplace raises concerns about its impact on working conditions. Thus, it can be argued, that it has negative implications for the working conditions, and this interfering with the right to favourable conditions at work. As it is technology's nature not to be human, the legal framework has difficulty in directly addressing this impact of wearables technology and reducing the risk of human rights violations.

Wearables continuously monitor work performance. This could offer companies reasons to overuse fixed-term contracts by using the performance data to justify the contracts or to terminate employment (Stefano and Wouters 2022). EU Directive 1999/70/EC implements rules to prevent employers using repeated fixed-term contracts (Council of the European Union 6/28/1999). But the law has it limits. It is seen critical, that the directive is sufficient to protect employees from abusing the data and take advantages of it and thus, violating the human right to favourable working conditions and the right to work and as well right to non-discrimination (Stefano and Wouters 2022).

Yet, the Article 22 of the General Data Protection Regulation may offer legal protection because according to this, employees have the right not to be subject to a purely automated decision (GDPR, Article 22). Therefore, the company must find other reasons to terminate employment and can not only rely on performance data (GDPR, Article 22).

The Transparent and Predictable Working Conditions Directive (TPWCD) enables employees to demand employment that delivers safer and more dependable working

conditions. (European Parliament; Council of the European Union 6/20/2019). Nevertheless, it is unclear whether this provision will result in a significant improvement in working conditions and the effective protection of human rights, as companies are only obliged to provide a reasoned reply in writing (Stefano and Wouters 2022).

Wearable technology has technical privacy vulnerabilities, such as unauthorised third-party access to the wearable device or connected IoT devices. This can lead to violations of the human right to privacy and data protection including the free flow of information (Rodrigues 2020). Due to loss of personal data or exploitation possibilities from having sensitive data about individuals. The protection of the right to privacy is linked to several other human rights, including the right to freedom of expression and the right to information, so it is essential to respect and uphold this right (ECHR, 8; CFR, Article 8).

The principles of the General Data Protection Regulation are all based on ensuring the fundamental right to privacy and data protection, as pointed out in Chapter 3.1.3 (ECHR, 8; CFR, Article 8). The ePrivacy Regulation aims to strengthen the GDPR in this respect and to limit third party access, thus ensuring the fundamental right to data protection and reduce human rights impact.

The requirements in the GDPR for a legal basis, the principles of fairness, transparency are ensuring the protection of personal data for the employee. In addition, the principle of confidentiality and the proposed measures to uphold a certain degree of confidentiality are protecting personal data and employee's right to privacy.

Transparency requires informed consent of the employee. But even though the GDPR sets standards to perform a lawful informed consent, a mistake can occur. Failure to obtain informed consent, or insufficient consent from the data subject, may result in violations of personal data protection, privacy, and individual freedom in the processing of personal data (ECHR, Article 5; CFR Article 8). Loss of sensitive information can result in exploitation and limit the safety of employees if it is used by unauthorised person and consequently employee's safety.

Wearables raise concerns if a fully informed consent cannot be given by the employee due to the complexity of the technology and therefore harm the human right to privacy. In such a case, trained staff and a Code of Conduct can prevent serious negative consequences for the company and the employee and protect human rights.

Furthermore, the GDPR provides the data subject with the option to raise opposition at any time to the processing of data or the analysis and decisions made by AI-enabled

wearables (GDPR, Article 15). Hence, the control over the personal data and therefore their privacy remains with the employee. However, it is argued critically, that the data analysis and the decision taken by AI can be understood fully by the employee to oppose the decision taking by AI or the data processing. Hence, it can violate the right to data protection and privacy and right to free flow of information (Rodrigues 2020).

It can be said that the current legal framework around wearables is strongly focused on preventing harm on the right to privacy by governing their personal data and its processing and thus, reducing potential impact on human rights. Yet, there are issues that lead to potential human rights violations such as the complexity of technology and technical vulnerabilities leading to data loss and unauthorised third-party access.

Concerns are raised regarding the accountability and liability of technology in cases of damages, leading to potential human rights implications for fair trial and access to justice (ECHR, Article 6). Wearable technology may record conversations or interactions, which could later be used as evidence in a legal proceeding. However, the context surrounding these recordings may not always be clear, thereby creating the possibility of misunderstandings or misinterpretations during trial. The data collected through wearable technology is vulnerable to unauthorised access or hacking. If confidential legal discussions or trial-specific information is obtained by unauthorised individuals, it could compromise the impartiality of a trial and hinder an individual's ability to obtain justice. If wearables are used by legal professionals, including judges, lawyers, or court staff, there may be worries about conflicts of interest or biases introduced through the data collected or accessed via wearables. This could undermine the neutrality and fairness of the trial.

As wearables or AI-equipped wearables lack legal personhood, the issue of liability is raised, which in turn affects the fairness of the trial process. The current legal regulations are based on strict liability. Yet it must be seen critically that the employee has the possible tools to claim for compensation or the allocation of liability is fair (Rodrigues 2020).

Therefore, there are efforts to legally classify AI systems as subjects liable for possible damages. However, the European Union is cautious about this approach due to the significant risks associated with granting AI legal personality. Such a step could lead to abuse or inconsistent application (Siemaszko et al. 2021). Diamantis and Grant (2017), while acknowledging that granting legal personality to AI systems is possible,

consider that such legislative action is morally unnecessary and subject to legal problems (Bryson et al. 2017; Rodrigues 2020).

Moreover, the European Union highlights its commitment to upholding human rights and safeguarding individuals through the introduction of the proposal of the Corporate Sustainability Due Diligence Directive (CSDDD) (European Comission 2023a). This directive is a significant step towards conducting comprehensive sustainability assessments, which are essential for evaluating and managing the environmental, social, and governance risks and impacts associated with a company's operations. The European Commission highlights that the primary objective is to ensure environmental and social responsibility, maintain strong corporate governance, create a positive corporate reputation, and align with stakeholder expectations (Council of the European Union) . Adopting this directive means companies have to meet specific requirements, especially when dealing with human rights abuses and negative environmental consequences. This, in turn, helps improve the legal framework in relation to privacy and corporate responsibility.

In conclusion it can be argued, that implementing wearables into the workplace poses risks in violating the human rights. This risk is reduced by strictly adhering to EU regulations, especially the GDPR, as they are based on and seek to protect the human right to privacy and the fundamental right to data protection. Not complying with the regulatory framework may possibly include violating human rights. Nevertheless, there are other human rights that are not directly addressed by the legislation around privacy, such as the right to work, right to favourable conditions at work and the right to non-discrimination. The labour law in particular the working time directive and the convention to termination of employment aim to comprehend EU regulatory framework to prevent violations against these rights. Yet, an updated version of labour regulations and specific directives regarding AI are necessary, to enhance human rights protection and fully address all affected rights. Further conduct of a human rights due diligence can enhance the protection of human rights.

4 Privacy Implications of Wearables in the Workplace

Incorporating wearable technology in the workplace has severe privacy implications and potential privacy risks related to data processing by wearables and connected devices. A following framework presents potential privacy risks focusing on the technical aspects for privacy protection. Further, the effectiveness of instruments and principles within the European legal framework analysed in chapter 3.1 to address privacy risks are assessed. Then, recommendations are provided regarding potential actions the company can take to protect employees' privacy.

4.1 Privacy Risk Framework

Wearables and their IoT ecosystem, consistent of a mobile device and a data storage, are posing weaknesses for employees' privacy and data protection.

Therefore, a privacy risk framework related to wearable technologies is presented below to understand the privacy risks that arise in the data processing cycle. Since wearable technologies work closely with amounts of personal data, the impact relating privacy issues is crucial.

The framework provides an overview of the privacy risks arising from technical circumstances of wearable technology. The framework leans on Segura Anaya et al. (2018). Further, it points out technological requirements for wearables to mitigate privacy risks and protect employees privacy (Segura Anaya et al. 2018).

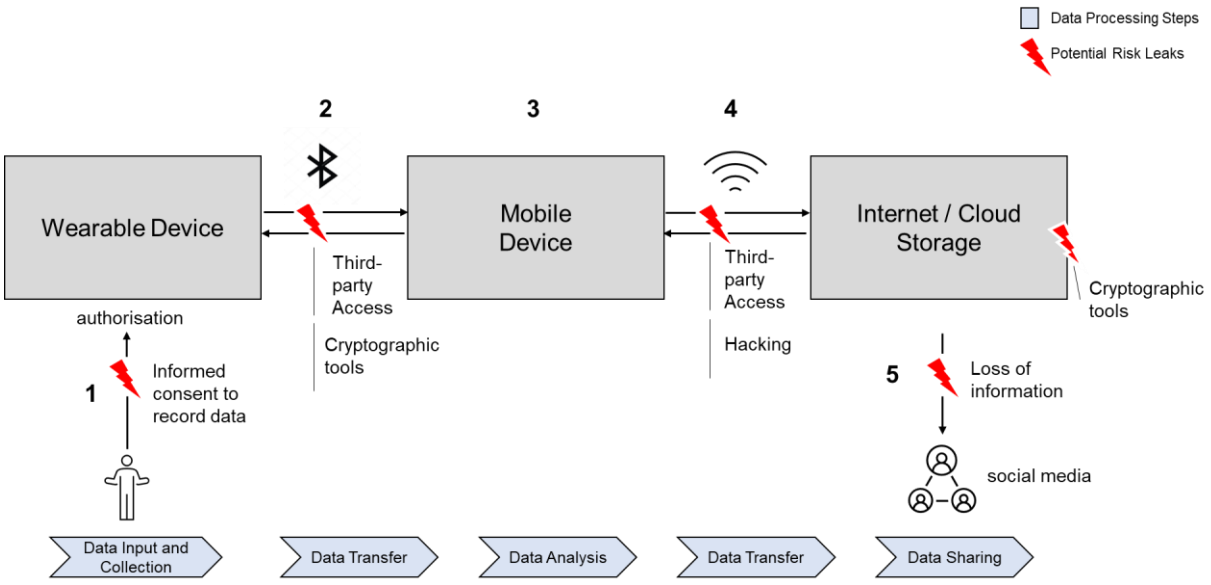


Figure 4-1 Privacy Framework based on Segura Anaya et al. 2018

Risks arising in data collection, giving informed consent & authorisation

1. The first step of the data processing involves the data collection from the wearable device. The data type collected from the wearables through the sensors is health data and therefore classified as highly personal (Maltseva 2020). The data contains information about for example the heart rate, activity status, or oxygen saturation. Because it is personal information, the data is classified as sensitive and confidential and potential loss of such information raises severe privacy concerns. That is why data processing of personal data requires a specific process (European Comission 2023d).

   The data is collected by the wearable device. It necessitates obtaining permission from stakeholders owning the device to record such data about the employee. Stakeholders are for example employers or project leads so the one owning the device. The permission is so-called informed consent. Getting the informed consent is crucial because the employee has the right to decide when and with whom to share collected data (Segura Anaya et al. 2018). It belongs to the fundamental right of the person to decide over the purpose of the data collected (European Union 2023). Privacy risks can arise if the informed consent is given without the full knowledge over the data processing of the personal data.

   Another risk is posed by authorisation issues of the device. Not sufficient secured devices with weak authorisation or a pin systems may lead to privacy vulnerabilities through poorly protected data on the device (Segura Anaya et al. 2018).

Risks arising in the Data Processing Cycle: Transfer, Analysis and Sharing

2. The wearable device transfers data to a connected mobile device for the data analysis and to facilitate data access and make it more visually clear to the user. The data is transmitted usually via a Bluetooth connection, which has potential vulnerabilities. First, insufficiently secured connections could allow unauthorised third party-access (Thierer 2014). Second, identifiable data poses privacy risk in case of data loss. So, during the data transfer process should the data be deidentified. That means separating the identity from the data and encrypting the data to reduce or eliminate privacy risks. For example, cryptographic tools can deidentify data (Wolf et al. 2016).

3. The next step in the data processing cycle is the data analysis from the mobile device. It can lead to create new information by combining raw data. This can invade the employee's privacy if the analysis reveals information about the employee that the employee has not given permission for. It is essential that the employee gives specific permission for the analysis (Segura Anaya et al. 2018).
4. The mobile device transfers data to a cloud storage via Wi-Fi connection. Data transmission via a Wi-Fi connection holds similar privacy risks to the Bluetooth transfer from the wearable device to the mobile device. The connection over WI-FI is vulnerable to third-party access without the consent of the user and to hacking. Here, identifiable data poses privacy risks as well in case of data leaks (Thierer 2014).
5. The last step in the data processing is the data sharing. The data sharing from the local storage to a cloud application with for example social media is revealing risk gaps as well. Data leaks or poorly secured storages can lead to a loss of information (Wolf et al. 2016).

A secure data process is crucial in terms of privacy and data protection. The framework identifies the interfaces where wearable technology could violate the data protection and where technical requirements are necessary to protect privacy and personal data of the employee. It highlights technical requirements to secure privacy when implementing wearable technology in a work environment.

4.2 Privacy Risks addressed by the Legal Framework

Examining the privacy risk framework, which outlines the privacy risks arising when implementing wearable technology in the workplace from a technological perspective, it will now be assessed whether the European legal framework adequately addresses the presented risks.

Risks arising in data collection, giving informed consent & authorisation

Due to the fact, that personal data is collected with wearables, the data protection regulation applies and aims to secure the sensitive data in data processing cycle (Wolford 2020).

The informed consent is necessary to lawfully process and record data (GDPR, Article 4). It gives the control and right to the employee deciding over the processing of their

data and to protect the employees right to decide over the purpose of their data collected (GDPR, Article 5). To secure the privacy and thus the personal data of the employee obtaining the informed consent correctly is crucial, as pointed out in the Privacy Risk Framework. Therefore, the GDPR defines that the informed consent must be given freely, specific, well-informed, and explicit (Wolford 2020).The GDPR further states that the data processing, including the purpose of the data collection and the insights into the data analysis, must be transparent for the employee to give legally accepted informed consent. Transparency enables individuals to give informed consent and gives them the opportunity to intervene in cases where they perceive a violation of their human rights (Sekalala et al. 2020). However, transparency is also important for lawfulness, to meet legal requirements, data processing must be transparent. Even though the General Data Protection Regulation clearly defines the requirements for the informed consent and transparency over the data processing cycle, it is argued critically that the company can ensure such a high level of transparency to understand the steps and the underlying analysis in the data processing to give informed consent. It raises concern about lawfully, fairness and transparent data processing and if it can be fully reached.

The lack of transparency in data processing and in the GDPR poses a privacy risk that the proposed AI Act aims to address and resolve. It aims to ensure higher transparency when introducing AI systems in the workplace to address the challenge of a lawfully consent. It provides a narrower definition of the scope of transparency, but it remains unclear whether it is possible in practice for the company to achieve even this more concretely defined level of transparency. However, including a code of conduct about wearable technology at the workplace could be beneficial for the principal of fairness and transparency. It supports clear communication of purpose and scope of use and analysis of the data and as well as the communication of values and rights related to the technology.

When it comes to data collection, the General Data Protection Regulation specifies that organisations should only collect data that is necessary for a specific purpose (GDPR, Article 5.1b). This principle, known as data minimisation, is designed to limit the unnecessary collection of data from wearables, reducing the potential for the use of large data sets.

As pointed out in the privacy framework, a non-secure authentication to access the wearable device poses a risk to lose or exploit employee's personal data. Thus, the GDPR states in Article 5.1f about the principle of confidentiality, that the data must be secured appropriately and further proposes concrete measures to ensure data security. Proposed measures are the security of wearables and the mobile device with two-factor authentication to reduce risk of unauthorised access to the devices. Additionally, should the wearable be capable of deidentify data to ensure from the beginning a secure data transmission (GDPR, Article 5.1f). In case of damages or loss of personal data, the consequences for the employee are less severe when the data is deidentified and there cannot be made direct conclusions to the identity of a person. Here, measures such as cryptographic tools are presented. Another measure is providing staff with training in data integrity and confidentiality. It can serve as a preventive measure against serious consequences in situations of technological failure or when encryption and other cryptographic tools are not feasible. This training may help implementing a mindset that ensures these principles are upheld in every operation involving data.

Risks arising in the Data Processing Cycle: Transfer, Analysis and Sharing

Privacy risks arising in the data transmission process are addressed by the GDPR through the principle of data confidentiality and data security (GDPR, Article 5.1f). Data confidentiality and integrity does not only include the data itself, but the data transmission processes, and thus electronic communications must be confidential as well. The GDPR and the ePrivacy regulations are ensuring the governing of connections and communications like Wi-Fi and Bluetooth connections within IoT systems. The regulations state that connections must be secured to ensure data protection and privacy for the employees. This will prevent third-party access or hacking attacks which means an invasion into the privacy sphere of the employee. In addition, the ePrivacy Regulation protects data loss through communication processes or data sharing, such as social media sharing. This efficiently reduces privacy risk regarding data transmission.

Another principle addressing privacy risks of wearables is the purpose specification (GDPR, Article 5.1b). The definition of a specific and explicit purpose and the requirements of being transparent to the data subject about the purpose, restricts data analysis of raw data. This can limit exploitation possibilities of the data analysis and may protect the abuse of personal data.

Furthermore, the principle of proportionality, including the limitation of the storage time, prevents potential privacy invasions due to data misuse (GDPR; Article 5.1c). The regulation states that data processing must be proportionate to the purpose and that the storage time is limited. Data must not be stored no longer than necessary for the stated purpose (GDPR, Article 51c). This can help reduce the privacy risks resulting from unauthorised access to the storage medium or accidental loss of data.

In Addition to necessary technical requirements to ensure privacy protection the company should offer appropriate training for the staff in data confidentiality and integrity to enhance privacy and reduce negative impacts in case of technological failures or data loss.

The provisions of the legal framework, in particular the General Data Protection Regulation, comprehensively addresses the privacy risks related to the protection of employees' personal data when wearable technology is used in the workplace. This framework focuses on a high level of confidentiality when dealing with such sensitive information. It is committed to limit data collection strictly in line with specified purpose and enforces restrictions on the duration of data storage, thereby minimising potential privacy risks. Furthermore, it provides clear guidelines to mitigate risks arising from unauthorised third-party access to portable devices or the data transmission links. Required measures include the implementation of two-factor authentication for device access and the use of cryptographic tools to deidentify data.

Nevertheless, it is seen critical, whether it is possible to implement the measures with the current technical conditions and if the wearable technology meets the requirements. Therefore, the next chapter discusses the concept of privacy by design and default to highlight the importance of cooperation between the developing company and the using company of wearables. Cooperations to develop the technology with privacy by default may efficiently mitigate possible violations of privacy rights and risks posed by technical features.

4.3 Privacy by Design & Default

While the principle “Privacy by design and default” does not directly belong to the data protection principles, it serves as an important guideline that emphasizes the need to implement data protection into the core of the development process (GDPR, Article 25). This is achieved by incorporating the principles into the technology development

process, promoting the idea that data protection should be an inherent, integral part and not an optional add-on when developing and implementing wearables.

Privacy by design means that a IT tool is built with automatically protection of personal data by default (Cavoukian 2009). This approach ensures that privacy remains untouched even without specific action by the user. The General Data Protection Regulation requires that organisations adopt a "by design and by default" approach to data protection in all their operations that deal with data (GDPR, Article 25). This proactive strategy aims to seamlessly integrate data protection into the architecture of systems or tools, making it an integral feature of core functionality. It promotes incorporating privacy into business practices and technologies without treating it as an add-on. In essence, prioritising privacy becomes the foundation for any new development and technology integration in the workplace.

Closely linked to this principle is the central concept of data security in the GDPR. All actions must prioritise data security by implementing specific technical and organisational measures. This aspect fits into the design and default principle, as every new technology integration requires such measures to align with the requirements of the GDPR.

In accordance with this principle, features of a wearable like two-factor authentication or data encryption become essential to comply with the principle of Privacy by Design and by Default. Consequently, wearables must uphold a certain level of data security throughout the entire data processing cycle to ensure compliance with the GDPR. The responsibility to follow the concept of privacy by design and default lies both within the company and within the technical design of the wearable. Embracing this concept not only ensures compliance but also fosters alignment with other privacy principles such as purpose specification and proportionality. When wearable technology is developed to collect only the data essential for a clearly defined purpose, it naturally aligns with the principles' requirements, without necessitating any adjustments on the part of the company.

Article 25 does not provide guidance for technological development but is intended to always keep privacy in mind and to provide legal incentives (Bygrave 2017). In addition, Article 25 lacks clarity on the goals and methods for achieving the "Privacy by design and default" and does not provide solid incentives to comply. Moreover, it hinders communication with those immediately involved in the design and development of such a system (Bygrave 2017).

Yet, the concept underscores the importance of appropriate technological requirements and the crucial cooperation of companies adopting and companies developing technology to ensure data protection and employees privacy at a top priority.

5 Case Study: Germany

For evaluating the efficacy of the integration of EU privacy and human rights regulations on a national level, the current legal framework in Germany will be outlined. This will include highlighting the similarities and differences with the European framework and identifying relevant supporting institutions.

Legal Framework	Institutions
Federal Data Protection Act (BDSG)	Work Council
German Telecommunication Act	Trade Union
	Data Ethics Comission

Figure 5-1 German Legal Framework

Germany was the first member of the European union to adopt and harmonise the legal framework for privacy at national level with the GDPR. While the GDPR holds supremacy and binds national legislation, it also allows for national laws to specify and elaborate on GDPR's provisions (European Comission). In order to comply with the GDPR, Germany introduced the Federal Data Protection Act in June 2017, which officially came into force in May 2018 together with the GDPR (Data Ethics Commission). The Federal Data Protection Act together with the GDPR, forms the basis of data protection laws in Germany (Federal Government of Germany 5/25/2018). In November 2019, a second act supplementing and modernising data protection law was introduced (Hornuf et al. 2023) At the European level, the ePrivacy Regulation was integrated into German law through the German Telecommunication Act with effect from December 2021, complementing the BDSG and thus the legal framework around privacy (Hornuf et al. 2023).

The BDSG is the main important data protection law protecting privacy in Germany as the GDPR is on European Level. The BDSG has similarities with the GDPR but as well distinct sections in the regulation.

The scope of the BDSG differ from and complement the GDPR. The BDSG applies to public and private authorities specifically setting a focus on businesses (Nebel 2022). This leads to more specific requirements for private companies in the BDSG in contrast to the GDPR which addresses data protection more generally (Nebel 2022). For instance, the BDSG specifically protects employee's personal data processing in the workplace context (BDSG, Section 26). The data processing for employment-related purposes states that the data processing is allowed to support decisions regarding hiring or terminating employment or if it necessary for the exercise or fulfilment of rights and obligations of the employee representation (BDSG, Section 26).

To proceed with this, the employee's consent remains essential. The BDSG like in the GDPR defines that the consent must be freely given (BDSG, Section 26.2). Furthermore, the BDSG emphasises the importance of this free choice, especially in lights of the possible imbalance of power between employers and employees due to their different positions of influence (as outlined in Chapter 2.2.1). The section 26 states, that "consent may be freely given in particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests." (BDSG, Section 26). By establishing these criteria for consent, it can mitigate the potential power imbalance that may arise from the use of wearable technology and data collection in the workplace. In particular, data processing in the context of the employment relationship is permitted under collective agreements (BDSG, Section 26.4).

In Addition, the BDSG is stricter in the appointment of a data protection officer (Nebel 2022). Companies are obliged to appoint a data protection officer if more than twenty people are permanently involved in data processing (BDSG, Section 38.1). The GDPR instead makes it obligatory for public authorities, if data is processed on a large scale and regularly and if specific data categories are processed like biometric data that makes a person identifiable (GDPR, Article 37 and Article 9). In contrast to the broad terms of the General Data Protection Regulation, the BDSG offers more concrete requirements for companies to comply with the regulation.

While Article 34 of the GDPR grants the Member States discretion regarding the permitted levels of fines, the BDSG provides for different levels of fines (GDPR, Article 34; BDSG, Article 42 and 43). Article 42 and 43 of the BDSG outline fines ranging up to €50,000, and in exceptional cases defined by BDSG Article 43, fines can go up to €300,000. On the other hand, the GDPR imposes fines of up to €20 million or 4% of revenue, whichever is higher (GDPR, 85.5; BDSG, Articles 42 and 43).

Another notable difference is the definition of non-monetary fines. The GDPR lacks a clear definition of non-monetary or "non-pecuniary" cases, whereas the BDSG precisely defines non-monetary damages and includes damages that are not quantifiable (Knetsch 2022).

Certain actions in relation to data violations are treated as a serious interference with personal rights in German legislation and are thus treated as criminal offences. Such actions are unauthorised access to a substantial amount of data or inadequate data security that allows third parties easy access, constitute criminal offences, and fall within the scope of the German Criminal Code (StrafGb, Article 202a-d). Insecure data transmission and connections are also criminal offences under the Criminal Code, which are explained in more detail in Article 303 (StrafGb, Article 303). Therefore, the legal framework in Germany underscores the gravity of data abuse and such violations of privacy due to the classification as a criminal act.

The BDSG complements the GDPR in the mentioned areas and introduces its own sections to close interpretation gaps within the GDPR. In contrast, the GDPR maintains a strict approach to fundamental privacy principles such as proportionality, transparency, and purpose limitation (GDPR, Article 5; BDSG, Section 67). It emphasises data security and confidentiality as well, without allowing significant room for different interpretations (BDSG, Section 64).

To summarise privacy measures under the German legal framework, the German Telecommunications Act works alongside the BDSG to regulate secure data communication and connections. This is similar to the ePrivacy regulation, which is implemented at the European level.

In contrast to the privacy framework, Germany's approach to artificial intelligence still lacks specific actions and regulations. In 2018, a strategy was put in place, and updated in 2020, which outlines a guideline to support a national AI-favoured economy (Federal Government of Germany 2020). The General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG) aim to guarantee secure data processing and privacy in context of AI and wearable technology. Nonetheless, a concrete legal framework besides of a strategy that guarantees the protection of privacy and human rights in context of AI and wearable technology sufficiently, is yet to be

established. Notably, Germany's federal structure means that each state approaches AI policy differently, raising questions (Jobin et al. 2021). This makes it more challenging to establish a binding policy equally applicable to all countries.
The AI Act and AI Directives currently remain under discussion at the EU level and have not yet been implemented, which could explain the absence of specific AI regulations in Germany. Implementing regulations and raising awareness of specific AI methodologies at European level may encourage subsequent national adaptations.

The legal framework around the protection of human rights in the digital age is a top priority in Germany (Nebel 2022; Data Ethics Commission). The German government actively supports the work of the UN Human Rights Council and is committed to further strengthening the role of the High Commissioner for Human Rights. In terms of human rights initiatives, Germany is one of the most active Council members in the European Union (Foreign Office Germany 2022).

Artificial intelligence and wearable technology have the potential to make discriminatory decisions or produce biased analyses due to the possibility of discrimination in the data. The General Equal Treatment Act (AGG) is designed to enhance employment relationships and application procedures by reducing these unwanted effects. AGG also prohibits discrimination in various areas, including the workplace (AGG, Article 2.1). However, it is important to understand the underlying implications of AI analysis and to ensure unbiased decision-making by the technology, similar to the challenges the EU is facing in discussing the AI Act.

The GDPR implements fairness principles and transparency requirements to reduce risks of discriminatory behaviour. The principle of transparency in the GDPR is reinforced in German law alongside the strict laws on general terms and conditions that also apply to data protection (Tribess 2023). Additionally, this law requires parties accused of discrimination to provide evidence of non-discriminatory activities and explain their decisions, which can pose challenges in the context of AI and its underlying processes (Tribess 2023).

In addition to legislation protecting privacy and data, Germany has reinforced its legal framework by several institutions.

Germany established a Data Ethics Commission. This Commission aims to ensure ethical incorporation of emerging technologies. Created in September 2018, the federal data ethics commission proposes and supports the government on legal and ethical questions related to information technology, including artificial intelligence (Data Ethics Commission). The commission plans to introduce forthcoming legislation that takes into account various perspectives, including technical, ethical, legal and sociological viewpoints, with the aim of creating a comprehensive framework for digital-era privacy and data security (Hornuf et al. 2023). It shows that the German approach emphasises the inclusion of different perspectives and that not only a legal framework needs to be put in place, but that more aspects need to be considered when working with data and technology in the workplace.

Furthermore, work councils in German companies have a strong impact on the national legislation around employees' rights. Work councils are playing a crucial role in the implementation of new technology in the workplace as stated in the Work Constitutions Act (European Comission). The Works Council Modernisation Act, applied in June 2021, even strengthen this position and their rights with the focus on projects regarding AI (Tribess 2023). Further, the new act states, that the employer must inform the work council about planning of the implementation of AI systems for work processes. This grants the council the authority to mitigate power imbalances between employer and employee and ensures that employee interests are taken into consideration. Furthermore, the council can regularly review and confirm the legal grounds of "legitimate interest" for data processing to maintain transparency and accountability.

In Germany, the trade union is another institution that strengthens the legal framework for employees. By formulating a comprehensive strategy for the integration of AI, trade unions can ensure a framework that protects privacy and human rights (Nebel 2022). Furthermore, they possess the power to campaign for the implementation of policies that conform to the fundamental values of human-centred technological design. Trade unions in Germany are integrated into strong networks, which gives them considerable power and influence. This can mean that they have a significant say in the processes of technological development and implementation (Haipeter 2020). Additionally, their national and works council collaborations allow them to make a far-reaching impact on a nationwide scale and within companies at an institutional level.

Germany has a legal framework concerning privacy and human rights, demonstrating a strong commitment to the European Union and the fundamental rights of citizens and employees. Nonetheless, the regulations for AI are currently inadequate. Germany's current approach to data protection and adapting new technologies involves a framework that strongly emphasises ethics. This is demonstrated by the establishment of a data ethics commission, which intends to show Germany's commitment to this area. In addition, the protection of employees' human rights in the digital age is supported by bodies such as trade unions and work councils. This approach could serve as a model for other countries to adopt in their efforts towards privacy protection.

In terms of future prospects, it is essential to enhance a more comprehensive legal framework in place that explicitly addresses the issue of AI. There is also a need for institutional strengthening and regular strategic meetings between organisations, work councils and trade unions as part of an ongoing process when implementing new technologies. It is also important to adapt a perspective that regards new technologies and their rapid development as a process. It is essential to regularly monitor and adjust the AI strategy accordingly, instead of solely relying on regulations (Krzywdzinski et al. 2023). To enhance their participation, Germany could broaden the understanding of digital processes among work councils (Haipeter 2020). Furthermore, the foundation for assuring that the roll-out and expansion of innovative technologies are competitive and beneficial to the economy is the creation of supportive policies. As Germany has underlined in its AI Strategy 2020, the objective is to have a positive influence on the economy (Federal Government of Germany 2020)
Yet, it's debatable whether the current framework is robust enough to balance the demands of competitiveness with ethical and regulated AI environments (Krzywdzinski et al. 2023).

6 Envisioning a Comprehensive Future Framework

The remaining legal and ethical challenges are outlined in the following section. Additionally, a comprehensive framework is presented, which adopts a multi-stakeholder approach to implement these challenges and protect privacy and human rights in the workplace through the use of wearable technology and AI.
This framework is followed by an outlook on the significant factors required for successfully integrating wearable technology into the workplace

6.1 Legal, Technical and Ethical Challenges

Chapters 3.1.3 and 3.2.2 analyse the instruments in the European legal framework and their impact on the protection of employees' privacy and human rights. The evaluation considers the impact on human rights and privacy risks, determining the appropriateness and adequacy of these tools to address the research questions (Chapter 4 and 3.2.2). Identifying the remaining challenges assists in identifying areas that may be insufficient and could be improved to enhance the protection of employees' rights.

Implementing wearable technology in the workplace is ruled by a legal framework around privacy and human rights. Especially the European framework analysed is popular for being one of the taffest worldwide. However, the existing regulatory system lacks provisions to protect employee rights and prevent harmful ethical effects resulting from the use of wearable technology. Consequently, legal, and ethical challenges persist in the adoption of wearable technology in the workplace.

In the European Union's legal framework, the GDPR states the principles of lawful, fair, and transparent data processing. There are concerns regarding the level of fairness and transparency achievable to protect privacy and human rights sufficiently, particularly with regards to equality and the right to non-discrimination. The GDPR does not concretely state the scope of transparency or fairness and leaves room for interpretation in the definition of these terms. Although the AI Act aims to bridge the gap and complement the GDPR in defining the scope of transparency, it is not enough to solve the difficulty of understanding the underlying processes of how and why the AI system made a certain decision and the algorithm behind a data analysis. This raises the question whether the company and employee can understand these technical processes completely to fulfil the transparency principle and provide legally informed consent. The informed consent is dependent on the information provided by the company to the employee, who can either accept or refuse the terms of data processing. It is unclear whether wearable technology can achieve the necessary level of transparency to comply with the transparency principle. Additionally, due to the complexity of the technological processes, it is critical to assess whether the employee or the company acting as data controller can understand all the underlying processes and the decisions made by the system and can object to the decisions made. Meeting these technical requirements is essential to ensure transparency and avoid potential violations of privacy. Moreover, with the vague definition of fair data processing in the legal framework, the company must find a way to ensure that it is fair to the employee. This raises ethical

concerns about whether the rules are adequate to guarantee that the company acts fairly and is not just trying to improve its business results. Achieving fairness at all stages of data processing remains a challenge when introducing wearables in the workplace.

Further, the ongoing challenge of finding a legal basis for the processing of personal data collected through wearable technology in the workplace has been shown to be significant and complex. Establishing a valid legal basis grounding it on “legitimate interest” is currently the solution under consideration but is seen critical. Balancing the rights of the data subject and controller is crucial for avoiding violations or compromises of human rights of employees. Justification of the legal base of "legitimate interest" for allowing data processing continues to be a difficult task.

Another remaining challenge is the issue of liability. Legal liability is a pressing concern currently under discussion, with unresolved risks and uncertainties presenting a challenge to the feasibility of holding AI accountable and if the allocation of responsibility is fair. The current liability directives are not sufficient, which is why the EU commission is currently deliberating on an AI Liability Directive to help protect companies, mitigate AI-related risks, and define compensation claims more clearly. A new directive may potentially reduce the immediate liability for both the company and its employees by putting it on the developer of the AI system. Moreover, it includes compensation for both material and immaterial damages. However, it remains questionable how effective this will be in practical terms. Can wearables be held legally responsible? There is an ongoing debate on whether it is reasonable to assign legal responsibility to AI systems or to grant them legal personality. However, there are several uncertainties and potential risks that need to be resolved initially. Ensuring legal liability is a difficult task but with crucial impact on protecting the human rights.

Going along with the aspect of accountability for damages, assuming responsibility for automated decisions is essential. Within the legal framework, accountability implies that decisions, whether based on AI and wearable analytics or proposed AI decisions, are difficult to challenge and rarely challenged. The GDPR does not provide sufficient protection against sensitive inferences made by wearables and artificial intelligence systems, or against challenging decisions made based on such inferences. This issue could potentially be addressed by the introduction of a “right to reasonable inference” (Wachter und Mittelstadt).

The present European legislation lacks specificity concerning the effects of AI on human rights and privacy. To address this issue and enhance the legal framework around wearables and AI, proposed directives and acts are under discussion.

To comply with legal requirements, technological specifications are crucial and must be met. These specifications are designed to uphold key principles outlined in the GDPR, such as purpose limitation and data minimisation. The regulations emphasize collecting and analysing only what is necessary for a specific purpose, maintaining data quality to prevent misleading analysis, and basing decisions on accurate data. Alongside these regulations, technical features serve to ensure optimal protection of personal data:

- Ensure regular deletion of data from storage and after a specified period to comply with the principle of storage limitation
- Ensure data confidentiality by using secure data connections, addressing the ongoing challenge of protecting data from third-party access
- Establish secure authentication processes for accessing wearables and IoT systems, enhancing privacy protections
- Secure data transmission and connections

It is however important to note that there are legitimate questions about the adequacy of current authentication methods, such as two-factor authentication and cryptographic tools, in securing both data and wearable devices. It is essential to recognize that while technical conditions can be advanced and improved, their limitations must also be acknowledged. AI, for example, lacks the ability to engage in discussions, express emotions, or act without intent - qualities that define human behaviour and distinguish us as individuals.

Additionally, compliance with labour rights, favourable working conditions, and the right to disconnect can be improved by incorporating precise technical requirements. To achieve compliance with these rights, technical conditions and design and default settings of wearables should be considered, as per Article 25 of the GDPR, which establishes the principle of data protection by design and default settings. Technical modifications could besides of their beneficial effects on the protection of personal data, prevent wearables from disrupting workers during their breaks by sending alerts about inactivity or work. However, there are uncertainties about the feasibility of these adjustments and the availability of such features. Furthermore, the GDPR does not

specify any measures for technical adaptations to comply with this principle. Consequently, the feasibility of technical requirements and their implications for privacy and human rights remain challenging.

The legal framework and regulations are unable to protect employees from the loss of data caused by physical device loss. However, the legal framework establishes measures to mitigate the consequences of such privacy risk for employee. Measures such as encrypted data and authentication security aim to protect employee data and privacy.

The increasing use of technology in the workplace may result in dehumanisation of the workplace, leading to unfavourable working conditions and negatively affecting employee well-being and performance. As technology is missing the human touch and its primary aim is to promote efficiency, addressing such issues may not be trivial. In addition, the drive for technology efficiency could unintentionally lead to discrimination and thus violate human rights. A potential concern is that an algorithm that analyses data with bias may produce discriminatory outcomes. It is uncertain whether algorithms can be entirely objective given their reliance on human input. Current research and development continue to address the questions of whether humans are free from bias, how to create an unbiased algorithm, and how to reduce discriminatory outcomes of automated decisions.

The complexity of defining the aims and scope of a global regulation has resulted in unresolved legal challenges and gaps in interpretation. The challenges of ensuring transparency and fairness are not only brought to light, but also the notion of “privacy by design and default” as described in Article 25 points out this difficulty by being vague and leaving room for interpretation. This leads to consideration of the suitable level of detail and whether the law should operate primarily as a framework, setting out goals and motivations, or whether it should offer exact guidelines for action. Given the argument that Article 25 serves more as a guiding principle than a comprehensive development guide, it is essential to evaluate whether it guarantees the protection of data and employee privacy or merely promotes these considerations to be prioritised in the thoughts and discussions of developers and data controllers (Bygrave, 2017). Perhaps the inclusion of a development guideline, the provision of more specific details in Article 25 to avoid mistakes, and the provision of concrete instruments and tools to facilitate compliance by companies would improve the current framework. Such a guideline can

address and facilitate the principles of ensuring data security and confidentiality, establishing a secure data connection, encrypting data, and thus meeting technical requirements and compliance with the regulatory elements.

A narrower definition of legislation can therefore be beneficial, but it can also hinder change processes or developments. Changes in labour markets and corporate structures are part of digitalisation and transformation. Legislation should not hinder transformation and change, but only regulate it appropriately, which raises the question of how rights can be protected while maintaining freedom for change.

In addition to the technical criteria and legal limitations outlined by the European framework to protect privacy and human rights, there are ethical challenges remaining when implementing wearables in the workplace.

The use of monitoring devices such as wearables in the workplace may cause employees to feel that their privacy has been invaded. This perception of a privacy violation can reduce motivation and hinder creative thinking. Given that individuals have different privacy thresholds, legislative measures to ensure comprehensive privacy coverage pose a significant challenge.

Regulatory mechanism aim to limit excessive monitoring and reduce the risk of employees feeling violated by emphasizing principles such as purpose limitation and proportionality. These regulations aim to provide employees with control over the processing of their personal data by informing them of their rights and promoting transparency in the processing procedure. Informed consent and commitments to transparency are essential regulatory measures for personal data processing. This could decrease the sense of continuous monitoring and improve individual autonomy and freedom. However, it remains unclear whether these measures are sufficient to address employees' common perception of being monitored. Further academic research is needed to fully assess this issue and outline potential strategies for improvement.

After assessing the current European legal framework, it can be said that it is robust in protecting data and privacy of employees in the context of wearables. However, there are still legal challenges and shortcomings in the regulations. Additionally, there remain technical and ethical challenges when implementing such technologies in the workplace to ensure full privacy and human rights protection.

Therefore, in the following, solutions are proposed to enhance the legal framework and address challenges. Since the environment surrounding AI and wearable technology is so complex, a comprehensive approach is necessary to fully tackle all remaining challenges and create a comprehensive framework to support the progress of such technologies within organisations. Thus, a multi-stakeholder approach has been proposed to address ethical, legal, and technical issues and create a comprehensive framework for the future implementation of wearables in the workplace. The proposed approach aims to ensure objectivity and clarity in the evaluation of these devices, while maintaining a balanced perspective of the issues and stakeholders' interests involved.

6.2 Multi-Stakeholder Approach

To address the complexity of issues and interests when implementing wearables and their IoT systems in a workplace, a multi-stakeholder approach is proposed. It can support setting ethical standards and address potential legal shortcomings and sets a basis for assumptions on how to foster a successful sustainable incorporation of wearables in the workplace (Will 2015).

A multi-stakeholder approach refers to a strategy that involves all groups, such as governments, organisations, companies, and institutions, that have a role to play in a particular outcome. This approach ensures that all interests and parties are represented and may promote sustainable solutions and a comprehensive framework around, for example, the approach to technology adoption like in this context (Will 2015). This approach is as well established within the legal framework as an action. To achieve the objectives of the CSDDD and reduce human rights violations, a multi-stakeholder approach is proposed (European Comission 2023a).

Building on the conceptual model outlined in chapter 2.3, the following chapter presents a more comprehensive framework that considers the interests of all stakeholders. An overall strategy needs to be implemented in the organisation to put employee rights at the centre, as well as promoting the appropriate implementation and development of new technologies such as wearables.

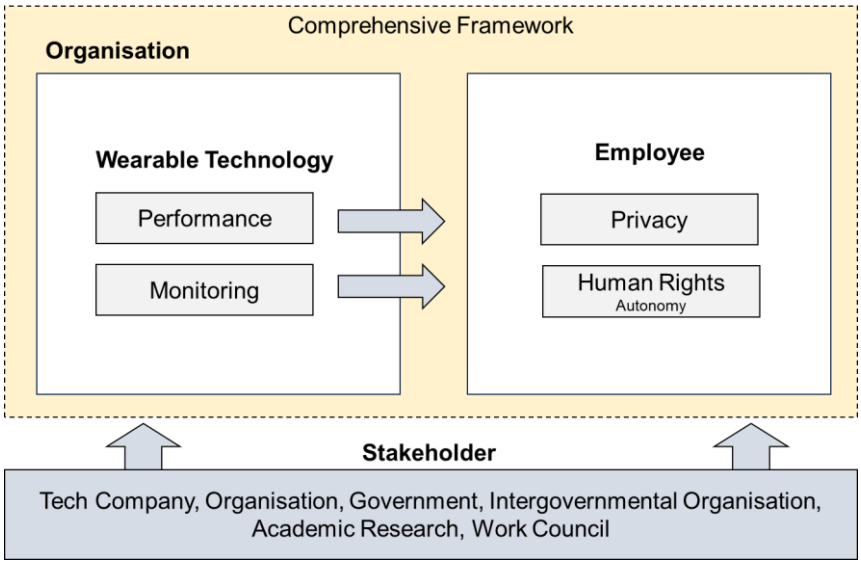


Figure 6-1 Conceptual Model: Comprehensive Framework

The following section will elaborate on possible actions that stakeholders can take to enhance a comprehensive framework. Additionally, proposed legal and ethical aspects to improve the comprehensive framework in the future are presented in order to address the remaining legal, technical and ethical challenges identified in chapter 6.1.

Organisation

As organisations are the ones implementing wearable technology, there are several approaches to improve the adaptation of technology and protection of rights. Future approaches could implement wearable technologies as part of an overall business strategy. Privacy and the protection of human rights could even be part of the corporate social responsibility (CSR) and thus be central to the strategic direction of the company and to the improvement and ethical framework. Corporate social responsibility involves a company's commitment to act ethically, responsibly, and sustainably in all aspects of its business, including its interactions with employees, stakeholders and the environment. This demonstrates a strong sense of commitment to, and even supports, a sustainable approach to technology adoption and development. The implementation of corporate social responsibility can include a code of conduct for such technologies. A code of conduct is typically considered a fundamental component of CSR. It is a set of policies and principles that describe the expected behaviour and ethical standards of the organisation and its employees. It provides a framework for responsible business practices, guides decision-making and ensures that actions are consistent with ethical and societal expectations.

Implementing a code of conduct for wearable technology in the workplace could be beneficial in protecting privacy and human rights by supporting the principles of fairness and transparency. It could define and explain the detailed use of wearables and their IoT system, provide clear communication about the purpose and scope of data analysis, and communicate the values and rights associated with the technology. Whilst not legally binding, various ethical guidelines and codes of conduct, these guidelines aim to ensure transparency, fairness, and accountability in the use of technologies which can have a positive impact on employees' perceived privacy. Such measures can reduce resistance and increase trust, thereby mitigating any negative effects related to the feeling of being monitored.

To assess the impact of technology implementation on human rights in the workplace, conducting a human rights due diligence is a useful tool (Wagner 2016). Companies can conduct comprehensive human rights due diligence to evaluate and comprehend the extent of human rights risks in the operation of AI systems and wearables (European Comission 2023a). This also helps in avoiding unintentional violation of legal requirements. The assessments examine the specific and potential direct and indirect impacts on individuals when implementing such technologies (Wagner 2016). By conducting due diligence, companies ensure that they don't violate human rights and meet the requirements of legality, necessity and proportionality of data processing and technology use. To pass the due diligence, any restrictions placed on the right to privacy must be lawful, necessary, proportionate, and comply with other rights.

To assess the privacy implications of implementing technology in the workplace, a privacy impact assessment can provide insight into these implications, and the company can then take steps to prevent privacy impacts and violations. A Privacy Impact Assessment (PIA) is a systematic assessment that helps organisations identify and mitigate privacy risks associated with the collection, analysis and storage of personal data (Clarke 2009). The goal of a PIA is to ensure that privacy considerations are integrated into the design and implementation of technology. PIAs are essential tools for ensuring that privacy is considered from the early stages, thereby promoting a privacy-centric approach to data processing (Clarke 2009).

Further actions that the company can take include holding regular assessments and meetings to ensure that the impact of the technology aligns with the company's

interests and the rights of its employees. It could be argued that it would enhance fairness and demonstrate the company's awareness of its employees' rights. This approach may lead to better protection of employees' rights and interests, thus improving the adaptation rate and enhancing employee well-being. Furthermore, it supports the justification of the legal basis of legitimate interest in data processing to ensure constant lawful data processing by balancing interests, as required when applying this legal basis.

In addition, it can be crucial to appoint a data protection officer. Such an officer would monitor critical aspects such as regular software updates and careful data deletion checks, ensuring that the company's technology remains up to date and effectively mitigates data risks and meeting compliance requirements.

Furthermore, the organisation can improve its data security measures by providing staff training on data confidentiality. This training will ensure that employees are adequately equipped to handle situations in the event of a data loss.

The main goal of the company is balancing wearables in the workplace. Mitigating potential power imbalances requires a balance between leveraging wearable technology for organisational benefits like performance and monitoring while respecting employees' rights to privacy, autonomy, and fair treatment. Clear communication, transparent policies, and ethical use of wearable data are essential to uphold a healthy work environment and prevent an unequal distribution of power.

Tech Company

Technology firms, especially those leading the way in wearable technology and IoT systems, have a crucial function. They create, design, and ensure that the technology meets the latest standards, ensuring accurate data collection. These companies play a crucial role in the development and verification of wearable privacy applications. They integrate features such as two-factor authentication, encryption and data deidentification for secure data transmission and enhanced data confidentiality. They can further invest into sustainable progress and environmentally friendly technologies and by that improving environmental impact.

Additionally, they continuously improve algorithms and AI systems to eliminate biases and facilitate transparent decision-making. Increased transparency in AI-driven decision-making processes improves privacy for employees. Collaborations between technology firms and organisations using wearables can be beneficial, ensuring that

the technology adheres to the workplace's specific requirements while maintaining its privacy and security standards. There are already significant initiatives by companies to find ways to develop unbiased AI, and to find out the processes that make AI decide the way it does.

Government

The government can establish clear regulatory frameworks and standards for the use of wearable technology in the workplace. In the future, further legal challenges such as liability issues including determining the legal personality of AI, can be addressed by the government. Additionally, the government could assess the feasibility and practicality of incorporating a right to inference within the existing legal framework. In collaboration with academic research and IGOs, a more effective regulatory structure could be established by solving the ongoing open questions.

The government can encourage the successful and sustainable integration of wearable technology into the workplace by providing a supportive regulatory environment, financial incentives, and facilitating research and development, which would benefit both companies and employees.

Intergovernmental Organisation

Intergovernmental organisations, such as the International Labour Organisation, have a crucial role in addressing remaining challenges when implementing technology in the workplace. These organisations have broad responsibilities to promote development, collaboration, and standardisation across the EU Member States. They can encourage the adaptation of wearables and protect employees' rights by establishing guidelines and standards for the implementation of technology. IGOs can influence current labour laws on issues of inequality in the workplace, to protect the right to work and security against rising unemployment, and thus to protect workers from significant changes in the labour market. Ensuring that labour laws remain up-to-date is an essential responsibility of IGOs. Additionally, IGOs can contribute to the exchange of methods and knowledge gained from experience to enhance the ongoing progress in implementing and developing technological frameworks amongst member countries and institutions.

Academic Research

Academic research can aid in the technical advancement of wearable technology by comprehending how employees interact with technology and their expectations. This

helps in designing and customising wearables to meet specific requirements. In addition, it can examine the impact of wearables in the workplace on health and safety on employees or the impact of wearables on performance, to gain more insights into risks and opportunities and balance them better. Additionally, further research can explore privacy and ethical impacts to better address remaining ethical and legal challenges in protecting employees' rights. Finally, evidence-based recommendations can contribute to creating guidelines that ensure responsible and ethical use of wearables.

Specifically, ongoing research proposes statistical methods to detect and evaluate discrimination by AI systems. These efforts could establish standardised procedures for assessing AI systems and their potential discriminatory consequences, and hence, reduce discriminatory effects of wearables and AI systems in the workplace (Wachter et al. 2021).

Work Councils

Work councils can prevent violations of employees' privacy and human rights. Regular evaluations and meetings with the management should be conducted to ensure that a wearable technology's impact aligns with both the company's and employee's interests, thereby promoting a balance in the use of wearables in the workplace. Additionally, work councils can promote the implementation of a code of conduct and challenge where and how technology is used in the company. They are crucial and essential institutions that safeguard employees in the workplace.

6.3 Successful Adaptation of Wearables in the Workplace

Successful integration of wearable technology in the workplace depends on various factors. The trust and acceptance of users are affected by privacy concerns and human rights implications. Overcoming these concerns is critical for effective wearable technology adoption, as user adoption plays a critical role in realizing the benefits associated with wearables in the work environment.

Establishing a strong legal framework, such as the GDPR, helps to address privacy concerns, thereby encouraging technology adoption. Offering clear communication about how data is used and giving employees a sense of control over their data, is critical to encouraging technology adoption. Transparency and informed consent

empower employees to control their personal data, ultimately reducing resistance to adopting technology in the workplace.

Balancing perceived risks and benefits plays a crucial role in an employee's decision to adopt wearable technology. Using wearables at the workplace does not only poses risks for data protection but as well risks impacting fundamental human rights like the right of privacy, and no discrimination.
For instance, employee monitoring with wearables at the workplace can increase workplace safety and performance but may lead to restricted employee autonomy and freedom when it comes to structure and organisation of their work. The possible quantification of performance encourages power imbalances between organisation and employee and may decreases the work engagement and perceived individual freedom. The analysis of employee data by the wearable and their connected IoT system may increase performance and efficiency and has positive impacts on productivity. Yet, the whole data life cycle presents privacy and security risks and the physical loss of the device is a hazard that should not be underestimated since a lot of devices have authentication issues which can lead to third-party access and misuse of information without consent of the employee and thus offers severe privacy risks.

It is essential to achieve a balanced implementation that weighs the benefits of data collection against considerations of privacy and human rights to successfully foster technology adoption.

Integrating new technologies into the overall business strategy can be a key factor for future success. Treating the implementation of wearable technology as a continuous process, instead of a one-time event, facilitates continuous adaptation, learning from mistakes and continuous improvement, thereby ensuring compliance with employees' rights. Including wearables in corporate social responsibility initiatives, for instance implementing a code of conduct can further support successful adoption. Providing staff training and assigning a data officer are crucial measures for data protection, preserving confidentiality, and ensuring the responsible handling of sensitive data, while raising awareness of the risks and opportunities associated with wearables.

To achieve successful implementation, collaborations provide opportunities to continuously improve technology by working on technical requirements and implementing new features for wearables with privacy by design as a priority. Academic research

and collaboration with intergovernmental organisations to establish standards will improve the framework around wearables and address existing challenges, including liability issues and gaps in labour laws.

In addition to legal and ethical considerations, companies should engage in regular internal assessments that include human rights due diligence and privacy impact assessments. These assessments ensure compliance with the law, prevent the violation of employees' rights, and promote lawful adaptation of technology.

To conclude, introducing wearables successfully into the workplace offers several benefits for the employee and the organisation such as enhancing workplace safety, preventing harm to employee’s health and increase organisational performance. Yet, mitigating data protection and privacy concerns and respecting human rights with a strong legal framework are critical to increase employee’s adoption and thus, foster a successful integration of wearables in the workplace.

7 Conclusion

In the following, the most important aspects will be summarized to answer the proposed research questions. Further, the limitations of this research will be outlined and potential areas for future research will be proposed. Lastly, a personal evaluation is presented.

Successfully integrating wearable technology and their IoT system into the workplace is essential for companies to remain competitive during the digital transformation era. The effective implementation of these technologies can provide valuable benefits, including improved performance and workplace safety.

However, it is crucial to acknowledge that wearable technology poses severe risks, particularly privacy risks and implications for human rights. The extensive collection and analysis of personal data pose several privacy risks to employees, and employee monitoring through wearables can reduce perceived autonomy and foster discrimination in the workplace as constant performance comparison occurs. Striking a balance between the risks and benefits of wearables is crucial for compliance, improving performance, promoting workplace safety, and successful wearable technology integration.

A conceptual framework is presented that aims to demonstrate the balance between the benefits of wearable technology, such as improved performance and monitoring, and the potential impact on workers, particularly in terms of their privacy and human rights like autonomy. To achieve a balanced approach towards the opportunities and risks, it is crucial to protect the rights of employees sufficiently. Therefore, this study analyses the existing European legal framework for protecting the privacy and human rights concerning wearable technology. The objective was to evaluate whether the legal instruments in place cover all the potential risks associated with wearables in a workplace, particularly violations of privacy and human rights.

The legal analysis of the European privacy framework shows a broad approach to addressing the privacy risks associated with the protection of employees' personal data through wearable technology. The framework concentrates on ensuring a high degree of transparency and fairness in the handling of personal data. It focuses on limiting data collection solely to its defined purpose and enforcing limitations on the duration of data storage, thereby mitigating potential privacy risks. Furthermore, clear guidance is provided to mitigate risks related to unauthorised third-party access to wearable devices or data transmission connections like Wi-Fi.

However, questions arise as to whether current technological capabilities are advanced enough to provide the full transparency of data processing that is required. Can the underlying processes behind automated decisions made by wearables or algorithms be fully understood to achieve a certain level of transparency? Additionally, there is a current debate on whether current authentication methods and cryptographic tools are sufficient to protect data and wearable devices. It is essential to acknowledge the potential for improving technical capabilities while also recognizing their limitations. For example, AI lacks the ability to reason, express emotion, or act with purpose.

An ongoing concern is the issue of legal liability for damage caused by wearables, particularly in the context of work settings involving AI. There is debate over whether AI can be granted legal personality.

Moreover, aims the European legal framework to address the human rights implications of wearables. Wearable devices can collect extensive data, which could lead to unequal treatment of employees once processed and analysed. This could result in discrimination based on performance data, potentially violating the right to non-discrimination and equality in the workplace. Moreover, technological progress greatly

influences work environments and changes within the job market, with possible consequences for labour rights, job security, and optimal work circumstances. While labour laws, the EU Convention on Human Rights and the GDPR attempt to address these issues, they do not include sufficient provisions for wearables and AI, limiting the effective management of such consequences in the workplace.

Ensuring privacy measures are implemented by design and default presents as a solution to reduce the discriminatory effects and enhance the protection of rights related to favourable conditions. Yet, utilising monitoring devices such as wearables in the workplace may cause employees to feel that their privacy has been invaded. It is uncertain whether the proposed measures in the legal framework are sufficient to mitigate the general feeling of surveillance among employees and thus reduce the human rights impact. The presence of legislation decreases the perception of privacy risks and increases control over personal data, thereby supporting adoption.

Despite this, the analysis highlights the crucial role of a comprehensive framework that encompasses both ethical and legal dimensions and recognises the interests of stakeholders. It is essential to create a specific framework to develop guidelines for wearables. Doing so guarantees employees' privacy in a world where technology is rapidly advancing and evolving.

The results are reflected in the case study at national level in Germany. The case study demonstrates that Germany has established a solid legal framework and uses the existing gaps in European legislation to its advantage for its own effective interpretations. Nevertheless, a gap still remains with regards to specific provisions on AI and its limitations. Furthermore, Germany reinforces its legal standards through various bodies such as trade unions, strong work councils and commissions such as the Data Ethics Commission. This demonstrates a commitment to recognising both the legal and ethical aspects of protecting privacy and human rights in the workplace, establishing a model for other member states to follow. It stresses the significance of examining workplace technologies from a comprehensive standpoint to tackle and minimise all challenges and risks.

Overcoming remaining challenges requires a multi-stakeholder approach to promote technology adoption. A comprehensive view of wearables in the workplace suggests considering both technological and legal requirements, as well as ethical aspects, to

protect the privacy and human rights of employees while maximising benefits for the company. Accordingly, this approach leads to the identification of key factors that drive the successful integration of wearable technology in the workplace. These considerations include the establishment of a strong legal framework, a balanced evaluation of potential risks and benefits, the integration of technology into the company's overall business strategy and, finally, the establishment of cooperations that can lead to the identification of solutions to ongoing challenges and risks. This can promote the successful and sustainable integration of wearables in the workplace.

The analysis has limitations. It focuses only on examining the privacy and human rights implications of wearable technology and AI-enabled wearables and their IoT systems. Further academic research is needed to explore the impact of other technologies and all AI systems used in the workplace, such as ChatGPT. Furthermore, it should be acknowledged that the scope of wearables considered in the analysis is clearly defined. However, it should be noted that these are only examples and that there are more wearables used in business operations.

Another aspect is that the analysis does not involve intellectual property rights as it is often a point of discussion with AI. In this case, AI wearables serve as a tool to support employees with data, enabling them to make proposed decisions, but rarely create something unique on their own. AI is mainly used for data analysis, and employees can still intervene in the decision-making process.

Further academic research is required to fully evaluate the forthcoming AI regulations currently under discussion at the European level.

In my opinion, implementing appropriate monitoring and control measures can be beneficial to a company, as it is possible with wearables. This practice provides assurance that employment contracts are being met. In the current work environment, where many employees work remotely, resulting in more frequent breaks and often raising concerns about lower work morale, it is understandable and necessary for companies to implement some level of monitoring and control. It is important to strike an appropriate balance between preserving employees' privacy and autonomy and maintaining their trust in the company. In addition, the unstoppable trend towards an increasingly digitalised working environment requires companies to remain aware and adaptable. To ensure their competitiveness, the creation of a legal framework should be a priority in order to maintain Germany's and Europe's leading economic position.

Another aspect to consider is the impact of smartphones and social media on younger generations, who are growing up with such technologies. Familiarity with and understanding of technology among younger employees make the adoption and utilization of advanced technology smoother and can result in positive outcomes. However, there are also negative consequences resulting from a lack of awareness of privacy risks and the potential loss of sensitive information affecting personal privacy as a result of the everyday use of technology and the fact that people are often unaware of how much data they are sharing with a single click or by agreeing to terms and conditions. Just a small click is often not enough to make employees understand the extent to which their privacy can be violated if data is lost or misused. A robust legal framework could mitigate these risks, while staff training raises awareness of the significance of data confidentiality and security.

To conclude, adopting new technologies in the workplace is crucial to remain competitive and adapt to unavoidable change. Thus, companies should invest in a robust framework that protects employees, enhances benefits and enables the digitalised workplace.

Appendix

In the following is an overview of the Regulation citations for the current editions to search for cited articles and the official proposals and reports from the European Parliament or Council of Europe.

General Data Protection Regulation (GDPR):
Edition 2016/679, http://data.europa.eu/eli/reg/2016/679/oj

Proposal for the Artificial Intelligence Act (AI Act):
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

Proposal for the ePrivacy Regulation (or Regulation on Privacy and Electronic Communications):
will replace the current Directive 2002/58/EC
https://digital-strategy.ec.europa.eu/en/library/evaluation-and-review-directive-200258-privacy-and-electronic-communication-sector

Report on the Artificial Intelligence Liability Directive (AI Liability Directive):
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0064

Proposal for the New Product Liability Directive:
https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739341/EPRS_BRI(2023)739341_EN.pdf

European Convention of Human Rights (ECHR):
https://www.echr.coe.int/documents/d/echr/convention_ENG

European Charter of Fundamental Rights (CFR):
http://data.europa.eu/eli/treaty/char_2012/oj

European Labour Law

- Working Time Directive
  Directive 2003/88/EC, http://data.europa.eu/eli/dir/2003/88/oj
- Transparent and Predictable Working Conditions Directive
  Directive 2019/1152, http://data.europa.eu/eli/dir/2019/1152/oj
- Termination of Employment
  https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C158

Proposal for the Corporate Sustainability Due Diligence (CSDDD)
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0071

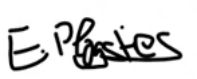
i. Declaration of Originality

I, Eileen Plogsties with the matriculation number 893882, declare my commitment to the principles of good scientific practice in the preparation of this Master's thesis.

I have written this thesis independently, using only the resources provided, and have indicated all passages taken from other works, either literally or as paraphrases.

I furthermore state that the electronic document submitted is an exact and unmodified copy of the content and wording of the printed version of the thesis. I give my consent for this electronic version to undergo plagiarism detection through analytical software.

Hamburg, 28.09.2023



8 References

Abd-Alrazaq, Alaa; AlSaad, Rawan; Shuweihdi, Farag; Ahmed, Arfan; Aziz, Sarah; Sheikh, Javaid (2023): Systematic review and meta-analysis of performance of wearable artificial intelligence in detecting and predicting depression. In *npj Digit. Med.* 6 (1), p. 84. DOI: 10.1038/s41746-023-00828-5.

AIDA Mandate (2022): Activity Report AIDA. Available online at https://www.europarl.europa.eu/committees/de/aida/home/highlights.

Albakjaji, Mohammed; Kasabi, Manal (2021): The right to privacy from legal and ethical perspectives. Available online at https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jnlolletl2424§ion=62.

Brey, Philip (2007): Ethical Aspects of Information Security and Privacy. In : Security, Privacy, and Trust in Modern Data Management: Springer, Berlin, Heidelberg, pp. 21–36. Available online at https://link.springer.com/chapter/10.1007/978-3-540-69861-6_3.

Bryson, Joanna J.; Diamantis, Mihailis E.; Grant, Thomas D. (2017): Of, for, and by the people: the legal lacuna of synthetic persons. In *Artif Intell Law* 25 (3), pp. 273–291. DOI: 10.1007/s10506-017-9214-9.

Bygrave, Lee A. (2017): Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements. In *OLR* 4 (2), pp. 105–120. DOI: 10.18261/issn.2387-3299-2017-02-03.

Cavoukian, Ann (2009): Privacy by design: The 7 foundational principles. Available online at http://jpaulgibson.synology.me/ethics4eu-brick-smartpills-teacherwebsite/secondarymaterial/pdfs/cavoukianetal09.pdf.

Ching, Ke Wan; Singh, Manmeet (2016): Wearable Technology Devices Security and Privacy Vulnerability Analysis. In *International Journal of Network Security & Its Applications* (8(3)), pp. 19–30.

Clarke, Roger (2009): Privacy impact assessment: Its origins and development. In *Computer Law & Security Review* 25 (2), pp. 123–135. DOI: 10.1016/j.clsr.2009.02.002.

Council of the European Union: Proposal for the Corporate Sustainability Due Diligence Directive. Available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0071, checked on 9/1/2023.

Council of the European Union (6/28/1999): Framework agreement on fixed-term work Directive 1999/70/EC. Available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0070, checked on 8/20/2023.

Data Ethics Commission. Available online at https://www.bmi.bund.de/EN/topics/it-internet-policy/data-ethics-commission/data-ethics-commission-node.html, checked on 9/2/2023.

DeLuca, Stefano (2023): New Product Liability Directive: EPRS: European Parliamentary Research Service. Available online at https://policycommons.net/artifacts/3450216/new-product-liability-directive/4250405/.

Dictionary Cambridge: Definition: Civil Liability. Available online at https://dictionary.cambridge.org/de/worterbuch/englisch/civil-liability.

Eager et al. (2020): Opportunities of artificial intelligence. Available online at https://www.sipotra.it/wp-content/uploads/2020/07/opportunities-of-artificial-intelligence.pdf.

ECHR (2023): Impact of the European Convention on Human Rights. Available online at https://www.coe.int/en/web/impact-convention-human-rights#/, checked on 8/8/2023.

European AI Strategy (2023): A European approach to artificial intelligence. Available online at https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence, checked on 7/19/2023.

European Comission: Employee Involvement - European Works Councils. Available online at https://ec.europa.eu/social/main.jsp?catId=707&intPageId=211&langId=en, checked on 8/2/2023.

European Comission: How should my consent be requested? Available online at https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/how-should-my-consent-be-requested_en.

European Comission: Reform of EU data protection rules. Available online at https://commission.europa.eu/law/law-topic/data-protection/reform_en.

European Comission (2021): Proposal for a Regulation laying down harmonised rules on artificial intelligence. Available online at https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence, checked on 8/10/2023.

European Comission (2023a): Corporate sustainability due diligence. Available online at https://commission.europa.eu/business-economy-euro/doing-business-eu/corporate-sustainability-due-diligence_en, checked on 8/29/2023.

European Comission (2023b): Data Protection. Available online at https://commission.europa.eu/law/law-topic/data-protection_en, checked on 7/3/2023.

European Comission (2023c): Types of Law. Available online at https://commission.europa.eu/law/law-making-process/types-eu-law_en, checked on 8/8/2023.

European Comission (2023d): What personal data is considered sensitive? Available online at https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en, checked on 7/3/2023.

European Court of Human Rights (9/3/1953): European Convention of Human Rights. ECHR, revised 8/1/2021, p. 62. Available online at https://www.echr.coe.int/documents/d/echr/convention_ENG#:~:text=The%20text%20of%20the%20Convention,force%20on%201%20June%202010., checked on 8/20/2023.

European Data Protection Supervisor (2023): Data Protection. Available online at https://edps.europa.eu/data-protection/data-protection_en, checked on 8/8/2023.

European Digital Strategy (2023): Proposal for an ePrivacy Regulation. Available online at https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation, updated on 9/15/2023.

European Parliament (12/1/2009): Charter of Fundamental Rights. CFR, p. 22. Available online at https://www.europarl.europa.eu/charter/pdf/text_en.pdf, checked on 8/18/2023.

European Parliament (2023): EU AI Act: first regulation of artifical intelligence. Available online at https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence, updated on 6/14/2023, checked on 9/1/2023.

European Parliament; Council of the European Union: General Data Protection Regulation (EU) 2016/679. Available online at https://eur-lex.europa.eu/eli/reg/2016/679/oj, checked on 8/1/2023.

European Parliament; Council of the European Union (8/2/2004): EU`s Working Time Directive 2003/88/EC,. WTD. Available online at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32003L0088, checked on 8/14/2023.

European Parliament; Council of the European Union (6/20/2019): Transparent and Predictable Working Conditions Directive 2019/1152. TPWCD. Available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L1152, checked on 8/20/2023.

European Union (2023): Data Privacy. Available online at https://gdpr.eu/data-privacy/#:~:text=Data%20privacy%20means%20empowering%20your,some%20of%20its%20key%20terms, checked on 7/27/2023.

Federal Government of Germany (5/25/2018): Federal Data Protection Act. BDSG, revised 6/23/2021. Available online at https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html, checked on 23.08.3023.

Federal Government of Germany (2020): Strategie Künstliche Intelligenz der Bundesregierung. Available online at https://www.bmwk.de/Redaktion/DE/Publikationen/Technologie/strategie-kuenstliche-intelligenz-fortschreibung-2020.pdf, checked on 9/11/2023.

Federal Office for Information Security Germany (2023): Wearables: So nutzen Sie Fitnesstracker, -armbänder & Co. sicher. Bundesamt für Sicherheit in der Informationstechnik. Available online at https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-

Verbraucher/Informationen-und-Empfehlungen/Internet-der-Dinge-Smart-leben/Smart-Home/Wearables/wearables_node.html, checked on 7/3/2023.

Foreign Office Germany (2022): Human rights – a cornerstone of German foreign policy. Available online at https://www.auswaertiges-amt.de/en/human-rights-acornerstoneofgermany/1034022.

Hackl, Cathy (2023): Wearables World.Will Apple Usher In An AI Future with AR Glasses? Available online at https://www.forbes.com/sites/cathyhackl/2023/05/05/wearable-world-will-apple-usher-in-an-ai-future-with-ar-glasses/.

Haipeter, Thomas (2020): Digitalisation, unions and participation: the German case of 'industry 4.0'. In *Industrial Relations Journal* 51 (3), pp. 242–260. DOI: 10.1111/irj.12291.

Han, Lu; Zhang, Qiang; Chen, Xianxiang; Zhan, Qingyuan; Yang, Ting; Zhao, Zhan (2017): Detecting work-related stress with a wearable device. In *Computers in Industry* 90, pp. 42–49. DOI: 10.1016/j.compind.2017.05.004.

Harvard Law School (2022): Intergovernmental Organizations. Available online at https://hls.harvard.edu/bernard-koteen-office-of-public-interest-advising/about-opia/what-is-public-interest-law/public-service-practice-settings/international-public-interest-law-practice-setting/intergovernmental-organizations-igos/, checked on 7/30/2023.

Hong, Jason (2013): Considering privacy issues in the context of Google glass. In *Commun. ACM* 56 (11), pp. 10–11. DOI: 10.1145/2524713.2524717.

Hornuf, Lars; Mangold, Sonja; Yang, Yayun (2023): Data Protection Law in Germany, the United States, and China. In : Data Privacy and Crowdsourcing: Springer, Cham, pp. 19–79. Available online at https://link.springer.com/chapter/10.1007/978-3-031-32064-4_3.

IAPP (2023): What is Privacy? International Association of Privacy Professionals. Available online at https://iapp.org/about/what-is-privacy/, checked on 7/27/2023.

International Conference of Data Protection (2018): DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE. 40th. Brussels.

International Labour Organisation (6/2/1982): C158 - Termination of Employment Convention, 1982 (No. 158). Available online at https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C158#:~:text=Convention%20concerning%20Termination%20of%20Employment,into%20force%3A%2023%20Nov%201985), checked on 8/23/2023.

Jacobs, Jesse V.; Hettinger, Lawrence J.; Huang, Yueng-Hsiang; Jeffries, Susan; Lesch, Mary F.; Simmons, Lucinda A. et al. (2019): Employee acceptance of wearable technology in the workplace. In *Applied Ergonomics* 78, pp. 148–156. DOI: 10.1016/j.apergo.2019.03.003.

Jobin, Anna; Guettel, Licinia; Liebig, Laura; Katzenbach, Christian (2021): AI Federalism: Shaping AI Policy within States in Germany.

Karale, Ashwin (2021): The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. In *Internet of Things* 15, p. 100420. DOI: 10.1016/j.iot.2021.100420.

Khakurel, Jayden; Pöysä, Simo; Porras, Jari (2017): The Use of Wearable Devices in the Workplace - A Systematic Literature Review. In Pietro Manzoni, Claudio Palazzi, Armir Bujari, Johann M. Marquez-Barja (Eds.): Smart Objects and Technologies for Social Good. Second International Conference, GOODTECHS 2016, Venice, Italy, November 30 – December 1, 2016, Proceedings, vol. 195. Cham: Springer (Springer eBook Collection Computer Science, 195), pp. 284–294.

Kingston, J. K. C. (2016): Artificial Intelligence and Legal Liability. In. International Conference on Innovative Techniques and Applications of Artificial Intelligence: Springer, Cham, pp. 269–279. Available online at https://link.springer.com/chapter/10.1007/978-3-319-47175-4_20.

Knetsch, Jonas (2022): The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases. In *Journal of European Tort Law* 13 (2), pp. 132–153. DOI: 10.1515/jetl-2022-0008.

Kokolakis, Spyros (2017): Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. In *Computers & Security* 64, pp. 122–134. DOI: 10.1016/j.cose.2015.07.002.

Krzywdzinski, Martin; Gerst, Detlef; Butollo, Florian (2023): Promoting human-centred AI in the workplace. Trade unions and their strategies for regulating the use of AI in Germany. In *Transfer: European Review of Labour and Research* 29 (1), pp. 53–70. DOI: 10.1177/10242589221142273.

Lamarre, Eric; Smaje, Kate; Zemmel, Rodney (2023): Rewired to outcompete. Available online at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/rewired-to-outcompete, checked on 9/18/2023.

Latonero, Mark (2018): Governing artificial intelligence: Upholding human rights & dignity. Available online at https://apo.org.au/sites/default/files/resource-files/2018-10/apo-nid196716.pdf.

Li, He; Wu, Jing; Gao, Yiwen; Shi, Yao (2016): Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. In *International Journal of Medical Informatics* 88, pp. 8–17. DOI: 10.1016/j.ijmedinf.2015.12.010.

Madiega, Tambiama André (2023): Artificial intelligence liability directive: EPRS: European Parliamentary Research Service. Available online at https://policycommons.net/artifacts/3450223/artificial-intelligence-liability-directive/4250433/.

Maltseva, Kateryna (2020): Wearables in the workplace: The brave new world of employee engagement. In *Business Horizons* 63 (4), pp. 493–505. DOI: 10.1016/j.bushor.2020.03.007.

Mettler, Tobias; Wulf, Jochen (2019): Physiolytics at the workplace: Affordances and constraints of wearables use from an employee's perspective. In *Info Systems J* 29 (1), pp. 245–273. DOI: 10.1111/isj.12205.

Miele, Francesco; Tirabeni, Lia (2020): Digital technologies and power dynamics in the organization: A conceptual review of remote working and wearable technologies at work. In *Sociology Compass* 14 (6), e12795. DOI: 10.1111/soc4.12795.

Mills, Adam J.; Watson, Richard T.; Pitt, Leyland; Kietzmann, Jan (2016): Wearing safe: Physical and informational security in the age of the wearable device. In *Business Horizons* 59 (6), pp. 615–622. DOI: 10.1016/j.bushor.2016.08.003.

Mitrou, Lilian (2018): Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?

Moeckli, Daniel; Shah, Sangeeta; Sivakumaran, Sandesh; Harris, David (2022): International human rights law. Fourth edition. Oxford: Oxford University Press.

Moßner, Julia; Bergmann, Linda (2019): Internet of Things (IoT) – Definition, Technologie und Anwendung. Available online at https://www.industry-of-things.de/internet-of-things-iot-definition-technologie-und-anwendung-a-878883/, updated on 3/3/2022, checked on 7/3/2023.

Motti, Vivian Genaro; Caine, Kelly (2015): Users' Privacy Concerns About Wearables. In. International Conference on Financial Cryptography and Data Security: Springer, Berlin, Heidelberg, pp. 231–244. Available online at https://link.springer.com/chapter/10.1007/978-3-662-48051-9_17.

Nebel, Michaela (2022): Germany - Data Protection Overview. Available online at https://www.dataguidance.com/notes/germany-data-protection-overview, checked on 9/10/2023.

O'Keeffe, Nathan; Scheid, Jennifer L.; West, Sarah L. (2020): Sedentary Behavior and the Use of Wearable Technology: An Editorial. In *International journal of environmental research and public health* 17 (12). DOI: 10.3390/ijerph17124181.

Oxford Dictionary (2023): Definition Wearable. Available online at https://www.oxfordlearnersdictionaries.com/definition/english/wearable_2, checked on 7/3/2023.

Patel, Vishal; Chesmore, Austin; Legner, Christopher M.; Pandey, Santosh (2022): Trends in Workplace Wearable Technologies and Connected-Worker Solutions for Next-Generation Occupational Safety, Health, and Productivity. In *Advanced Intelligent Systems* 4 (1), p. 2100099. DOI: 10.1002/aisy.202100099.

Philip Jansen; Stearns Broadhead; Rowena Rodrigues; David Wright; Philip Brey; Alice Fox; Ning Wang (2019): SIENNA D4.1: State-of-the-art Review: Artificial Intelligence and robotics.

Psychoula, Ismini; Chen, Liming; Amft, Oliver (2020): Privacy Risk Awareness in Wearables and the Internet of Things. In *IEEE Pervasive Comput.* 19 (3), pp. 60–66. DOI: 10.1109/mprv.2020.2997616.

Raso, Filippo; Hilligoss, Hannah; Krishnamurthy, Vivek; Bavitz, Christopher; Kim, Levin Yerin (2018): Artificial Intelligence & Human Rights: Opportunities & Risks.

Rodrigues, Rowena (2020): Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. In *Journal of Responsible Technology* 4, p. 100005. DOI: 10.1016/j.jrt.2020.100005.

Safavi, Seyedmostafa; Shukur, Zarina (2014): Improving Google glass security and privacy by changing the physical and software structure. In *Life Sciences* 11 (5). Available online at https://www.researchgate.net/profile/seyedmostafa-safavi/publication/265867348_improving_google_glass_security_and_privacy_by_changing_the_physical_and_software_structure.

Şandru, Daniel Mihail (2020): The Fairness Principle in Personal Data Processing. In *Law Review* (01), pp. 60–69. Available online at https://www.ceeol.com/search/article-detail?id=1035900.

Security, Privacy, and Trust in Modern Data Management (2007): Springer, Berlin, Heidelberg.

Segura Anaya, L. H.; Alsadoon, Abeer; Costadopoulos, N.; Prasad, P. W. C. (2018): Ethical Implications of User Perceptions of Wearable Devices. In *Sci Eng Ethics* 24 (1), pp. 1–28. DOI: 10.1007/s11948-017-9872-8.

Sekalala, Sharifah; Dagron, Stephanie; Forman, Lisa; Meier, Benjamin Mason (2020): Analyzing the human rights impact of increased digital public health surveillance during the COVID-19 crisis. Available online at https://www.ncbi.nlm.nih.gov/pmc/articles/pmc7762901/.

Siemaszko, Konrad; Rodrigues, Rowena; Slokenberga, Santa (2021): D5.6: Recommendations for the enhancement of the existing legal frameworks for genomics, human enhancement, and AI and robotics. Available online at https://www.diva-portal.org/smash/record.jsf?pid=diva2:1527337.

Stefano, Valerio de; Wouters, Mathias (2022): AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework.

Stein, Mari-Klara; Wagner, Erica L.; Tierney, Pamela; Newell, Sue; Galliers, Robert D. (2019): Datification and the Pursuit of Meaningfulness in Work. In *Jour. of Manage. Stud.* 56 (3), pp. 685–717. DOI: 10.1111/joms.12409.

Thierer, Adam D. (2014): The Internet of Things & Wearable Technology: Addressing Privacy & Security Concerns Without Derailing Innovation.

Tribess, Alexander (2023): Artifical Intelligence - Germany. Available online at https://www.globallegalpost.com/lawoverborders/artificial-intelligence-1272919708/germany-623281725, checked on 9/12/2023.

United Nation General Assembly (1948): Universal Declaration of Human Rights. UDHR, revised 217A.

United Nations (2023): Universal Declaration of Human Rights. Available online at https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Wachter, Sandra; Mittelstadt, Brent (2018): A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI: Center for Open Science.

Wachter, Sandra; Mittelstadt, Brent; Russell, Chris (2021): Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. In *Computer Law & Security Review* 41, p. 105567. DOI: 10.1016/j.clsr.2021.105567.

Wagner, Benjamin (2016): Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications. Council of Europe Report.

Will, Matthias Georg (2015): Privacy and Big Data: The Need for a Multi-Stakeholder Approach for Developing an Appropriate Privacy Regulation in the Age of Big Data. In *SSRN Journal*. DOI: 10.2139/ssrn.2634970.

Wolf, Christopher; Polonetsky, Jules; Finch, Kelsey (2016): A practical privacy paradigm for wearables. Available online at https://fpf.org/wp-content/uploads/2015/01/fpf-principles-for-wearables-jan-20151.pdf.

Wolford, Ben (2020): What is GDPR, the EU’s new data protection law? Available online at https://gdpr.eu/what-is-gdpr/.