Rising like a Phoenix: Emerging from the Pandemic and Reshaping Human Endeavors with Digital Technologies ICIS 2023

IS in Healthcare Addressing the needs of post-pandemic digital healthcare

Dec 11th, 12:00 AM

A Privacy Impact Assessment Method for Organizations Implementing IoT for Occupational Health and Safety

Stefan Stepanovic
University of Lausanne, stefan.stepanovic@unil.ch

Dana Naous
Faculty of Business and Economics (HEC), University of Lausanne, dana.naous@unil.ch

Tobias Mettler
University of Lausanne, tobias.mettler@unil.ch

Recommended Citation

Stepanovic, Stefan; Naous, Dana; and Mettler, Tobias, "A Privacy Impact Assessment Method for Organizations Implementing IoT for Occupational Health and Safety" (2023). *Rising like a Phoenix: Emerging from the Pandemic and Reshaping Human Endeavors with Digital Technologies ICIS 2023*. 14.
https://aisel.aisnet.org/icis2023/ishealthcare/ishealthcare/14

A Privacy Impact Assessment Method for Organizations Implementing IoT for Occupational Health and Safety

Completed Research Paper

Stefan Stepanovic
University of Lausanne
Rue de la Mouline 28
1022 Chavannes-près-Renens
stefan.stepanovic@unil.ch

Dana Naous
University of Lausanne
Rue de la Mouline 28
1022 Chavannes-près-Renens
dana.naous@unil.ch

Tobias Mettler
University of Lausanne
Rue de la Mouline 28
1022 Chavannes-près-Renens
tobias.mettler@unil.ch

Abstract

Internet of Things (IoT) technologies are increasingly being integrated into occupational health and safety (OHS) practices; however, their adoption raises significant privacy concerns. The General Data Protection Regulation (GDPR) has established the requirement for organizations to conduct Privacy Impact Assessments (PIAs) prior to processing personal data, emphasizing the need for privacy safeguards in the workplace. Despite this, the GDPR provisions related to the IoT, particularly in the area of OHS, lack clarity and specificity. This research aims to bridge this gap by proposing a tailored method for conducting PIAs in the OHS context, with a particular focus on addressing the "how to" aspect of the assessment process. The proposed method integrates insights from domain experts, relevant literature sources, and GDPR regulations, ultimately leading to the development of an online PIA tool.

Keywords: Internet of Things, Occupational Health and Safety, Privacy Impact Assessment

Introduction

It is now clear that the COVID-19 pandemic has left an indelible mark on work practices and has drastically changed our approach to Occupational Health and Safety (OHS). Internet of Things (IoT) technologies have emerged as powerful tools for monitoring, managing, and improving worker health and safety in the workplace (Mettler and Naous 2022). However, while IoT technologies have the potential to improve worker health and physical activity through real-time data and tailored feedback, they also create opportunities for companies to exploit worker data, particularly for productivity-related purposes (Castelluccia et al. 2018; Lupton and Michael 2017). As such, IoT technologies can be seen as ambivalent tools, simultaneously possessing beneficial and detrimental attributes, while also bearing a degree of complexity and opacity that can hinder effective control (Aanestad et al. 2018). This dual nature of the IoT in OHS underscores the need for careful decision making around privacy considerations when implementing such technologies in the workplace.

Addressing privacy concerns in an organizational setting is not merely a recommendation, but a legal requirement, as specified in Article 35 of the General Data Protection Regulation (GDPR). This article mandates organizations that use new technologies with potentially high risks to individuals' rights and freedoms to conduct a Privacy Impact Assessment (PIA) before processing personal data. The GDPR applies to all organizations based in the European Union (EU) that handle personal data and covers various facets such as data collection, processing, transfer, storage, and security. As of May 25, 2018, the GDPR imposes penalties for non-compliance, including fines of 4% of the organization's annual global turnover (Golightly et al. 2022). This regulatory framework extends its reach beyond the EU and has inspired the formulation of similar privacy regulations around the world. For example, the California Consumer Privacy Act (CCPA) in the United States and Brazil's new data privacy regulations were inspired by the GDPR (Akhlaghpour et al. 2021). In addition, other countries, including India, Japan, and Australia, are currently developing robust data privacy legislation. In Canada, the Data Privacy Act was enacted as an update to the previous legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA), facilitating seamless data sharing with the EU (Kounoudes and Kapitsaki 2020). Therefore, the importance of privacy as mandated by the GDPR can be considered as a landmark legislation that establishes the individual's right to privacy and as a holistic approach to privacy for IoT in organizational settings.

However, there is a lack of clarity in key provisions of the GDPR relevant to the IoT, as most of the recommendations on PIAs are not formalized, leaving room for subjective interpretation (Fabiano 2017a; Häikiö et al. 2020; Wachter 2018b). For instance, the methodology provided by the UK Information Commissioner's Office (2014) mainly offers general and abstract guidance on the privacy assessment process. Yet, it is crucial to consider the actual design of IoT systems in order to identify specific design flaws and security threats (Ahmadian et al. 2018). This lack of clarity and specificity is particularly problematic in the OHS context, where individuals tend to be more sensitive to risk perceptions when health data is involved (Lee et al. 2019; Vegh 2018). Furthermore, the perceived usefulness of the IoT is heavily dependent on its ability to respect individuals' privacy choices (Tawalbeh et al. 2020).

Therefore, the focus of our work is not only to determine "what to do" in terms of PIAs, but also to address the crucial question of "how to do it". We propose the development of a method for conducting PIAs that is specifically tailored to OHS. In this context, a method refers to a systematic, goal-oriented, and repeatable approach that provides clear rules, instructions, and standards for achieving defined objectives (Braun et al. 2005). Unlike models, which focus primarily on state descriptions, methods emphasize the specification of activities and the practical steps to be taken. More specifically, we propose to develop a framework for a PIA that will help organizations to objectively assess their compliance with GDPR regulations (which serve as a benchmark for data protection and privacy).

Against this background, our research question is: *How can organizations assess key privacy risks associated with the use of IoT in OHS, while ensuring compliance with GDPR principles?*

In order to formulate our PIA method, we intend to employ the Situational Method Engineering (SME) approach. The adoption of SME enables the construction of a comprehensive method by assembling pre-existing and reusable fragments of methods (Ralyté et al. 2003; Rolland and Prakash 1996). Our approach notably incorporates insights provided by domain experts, along with elements extracted from relevant literature sources and regulatory frameworks such as the GDPR. This method is then subsequently materialized into an online PIA tool for practical implementation.

The remainder of this paper is structured as follows. First, we briefly provide background information on PIA and GDPR principles. Then, we describe our research approach in the design of our PIA method (and its embodiment in a PIA tool) and discuss it. We conclude the paper with our formulation of limitations and opportunities for future research.

Background

Privacy Impact Assessment (PIA) and Key GDPR Principles

Article 35 of the General Data Protection Regulation (GDPR) outlines the requirement for organizations to conduct an assessment of the impact of their data processing activities on the rights and freedoms of individuals. This assessment, known as a Privacy Impact Assessment (PIA), follows a systematic risk management approach (Gonzalez-Granadillo et al. 2021; Oetzel and Spiekermann 2014). Its aim is to evaluate the potential effects of a system on privacy, while promoting trust and implementing the Privacy-by-Design principle. Privacy-by-Design refers to the philosophy of incorporating privacy considerations into the design specifications of various technologies (Cavoukian and Chibba 2009).

PIAs act as a preemptive warning mechanism to identify potential vulnerabilities during system development (Wright 2013). This concept originates from initial assessments used for Technology Assessment (TA) by the US Office of Technology Assessment (OTA). The term was gradually institutionalized in 1995 under Article 20 of the European Directive, mandating 'prior checking' against applicable standards, especially for sensitive information systems (Clarke 2009). In contrast to conventional risk management methods in organizations, PIAs offer a distinct perspective that prioritizes privacy concerns. This allows organizations to proactively address potential privacy risks that may be overlooked by broader assessment tools.

Typically, PIAs are conducted by actively involved program managers (such as project managers, legal experts, or IT professionals) (Tancock et al. 2013). Effective PIAs are often the result of individuals with strong project management knowledge and cross-disciplinary skills (Warren et al. 2008). Nonetheless, project managers need to understand their responsibilities under GDPR guidelines when embarking on programs involving sensitive data. It is imperative that they are equipped with the necessary data protection knowledge and skills to conduct competent PIAs. Consequently, PIAs serve as a proactive organizational tool that facilitates the management of potential data-related impacts. They also reflect a commitment to accountability and compliance (Oetzel and Spiekermann 2014).

Despite the existence of frameworks and guidelines for conducting PIAs since the early 2000s (Clarke 2009), the procedure remains challenging for emerging technologies. This is due to the number of stakeholders involved (e.g., various technical third parties) and the unpredictable nature of their business models (e.g., large amounts of data that can be used for multiple purposes) (Gonzalez-Granadillo et al. 2021; Vemou and Karyda 2018). To simplify the process, the Canadian government has made recommendations that divide the PIA into four main steps:

1) Project Initiation: This step involves defining the scope of the PIA and adapting the provided guidelines to the specific context of the project.
2) Data Flow Analysis: This step analyzes and describes the proposed business processes, architecture, and detailed data flows. The main objective is to outline the flow of personal information within the project.
3) Privacy Analysis: This phase examines the data flows in relation to relevant privacy policies and legislation. Questionnaires can be used as a checklist to identify key privacy risks or vulnerabilities associated with the project.
4) Report Generation: The final stage of the PIA process is to produce a comprehensive report based on the findings of the previous steps. This report evaluates the privacy risks and their potential consequences, and may propose remedies or mitigation strategies. In this sense, the PIA report serves as an effective communication tool for the various stakeholders involved in the project.

In order to construct a PIA, the GDPR provides a framework based on its core data protection principles outlined in Chapter 2, Article 5 (Regulation 2016). These principles serve as a solid foundation for conducting a PIA and ensuring data protection compliance (Fabiano 2017a; Wachter 2018b).

These principles include:

Lawfulness, Fairness, and Transparency: Personal data must be processed lawfully, fairly, and transparently, with individuals being informed about how their data will be used.

Purpose Limitation: Personal data should be collected for specified, unambiguous and relevant purposes and should not be further processed in a way that is incompatible with those purposes.

Data Minimization: Data collected should be adequate, pertinent and restricted to what is necessary for the intended purpose of processing.

Accuracy: Personal data must be accurate and, where necessary, kept up to date, with reasonable steps taken to ensure inaccurate or incomplete data is rectified or erased.

Storage Limitation: Personal data should be kept in a form that allows identification for no longer than necessary for the intended purpose, considering legal obligations and legitimate business needs.

Integrity and Confidentiality: Appropriate security measures must be in place to protect personal data against unauthorized or unlawful processing and accidental loss, destruction, or damage.

Accountability: Organizations are responsible for demonstrating compliance with the GDPR's principles and must have appropriate measures and documentation in place to demonstrate their compliance.

IoT for Occupational Health and Safety

IoT technologies are seen as a way to quantify workplace behaviors and environmental conditions (Mettler and Wulf 2019). A diverse range of devices, including smart watches/wristbands (e.g., Glance et al. 2016), smart clothing (e.g., Venkatesh 2017), or environmental sensors (e.g., Synnott et al. 2016) can be employed to gather real-time data. These devices are commonly designed to assist employees in monitoring various aspects of their physical health, such as sedentary behavior (Stephenson et al. 2017) or posture (Ailneni et al. 2019; Roossien et al. 2017). They may also provide insights into emotional health indicators like stress detection (Stepanovic et al. 2019), as well as environmental factors such as temperature and humidity variations (Nižetić et al. 2020).

Despite the potential benefits of IoT in detecting and preventing health issues, as well as promoting employee health awareness and proactive measures, the implementation of IoT health initiatives presents significant challenges concerning privacy. This stems from the sensitivity of health data and the continuous monitoring that is involved (Yassaee and Mettler 2017). Therefore, the extent to which IoT systems respect individuals' privacy choices has a significant impact on their effectiveness (Psychoula et al. 2018). Likewise, potential negative consequences associated with IoT implementations may hinder their widespread adoption (Brous et al. 2020). To address these concerns and recognize the importance of users' privacy rights, ongoing efforts are dedicated to redefining privacy issues and addressing concerns associated with the growing use of IoT and its associated services (Akil et al. 2020; Khan et al. 2016). As a result, organizations are encouraged to prioritize privacy risks assessments to effectively address these challenges (Wachter 2018b).

Research Approach

Methods are an important and recognized means of organizational engineering in information systems research. They provide detailed, goal-oriented descriptions of activities to be performed in order to solve a specific problem (Braun et al. 2005; March and Smith 1995).

In line with Braun et al. (2005), we have defined a method as a systematic approach used to perform specific tasks and achieve predetermined objectives, with the main elements presented in Table 1. As a concrete guideline for designing a PIA method, we follow a situational method engineering approach (and more specifically an assembly-based method engineering), as outlined by (Ralyté et al. 2003). The process involves (1) defining method requirements, (2) selecting appropriate method components, and (3) assembling these components into a coherent (new) method (Ralyté et al. 2003).

	Name	Description
Fundamental attributes of a method	Goal orientation	Methods strive for achieving specific goals
	Systematic approach	Methods possess a specific structure
	Principles	Methods are bound to design principles or strategies
	Repeatability	Methods can be repeated in different contexts
Fundamental elements of a method	Activity/procedure model	Task that creates a distinct (intermediate) output
	Role	Actor that executes or is involved in the execution of an activity
	Technique	Detailed instruction that supports the execution of an activity
	Tool	Instrument that supports the execution of an activity
	Defined Output	Specifies the outcome of each activity

Table 1. Method Attributes and Elements (Braun et al. 2005; Denner et al. 2018; Fridgen et al. 2018)

Overall Method Objectives and Requirement Specifications

The SME approach involves the explicit explanation of situations in which the method can be applied (Asadi and Ramsin 2009; Rolland and Prakash 1996). In fact, the design and construction of a method can be likened to other engineering activities, where certain contextual factors and requirements are provided, and an appropriate artifact that meets these requirements must be developed (Gonzalez-Perez et al. 2009).

The broad context (i.e., "when" and "why") of a PIA method for occupational health is outlined in the early sections of this paper. However, it is imperative to ensure that risks are rigorously assessed throughout the implementation of IoT in organizations. This requires that privacy is no longer considered as an abstract and overarching concept, but rather as a set of concrete risks associated with each layer of the IoT architecture, from the sensor level to the application level (*Activity 1*).This is consistent with the initial phase of a PIA process (as described in the Background section), which involves precisely defining the scope of the PIA.

We then gather insights through a focus group with OHS experts to map the flow of personal information in organizations (*Activity 2*). As indicated by Wright (2013), risk assessment is a somewhat subjective exercise. Therefore, it is beneficial to involve practitioners and experts to get their views. We also complement practitioners' views with a systematic literature review (*Activity 3*) to draw on the justificatory knowledge obtained from the existing literature and the GDPR.

The derived findings from the first three activities serve as the basis for the construction of the questionnaire, which is used in our PIA data flow analysis and data protection analysis. Finally, we integrate all these components into a PIA methodology for OHS, which is presented in the form of a prototype website capable of generating reports (*Activity 4*).

Design Activities and Elements

Activity 1: Breakdown of IoT Data Flow in Organizations

Technique: Activity 1 addresses the need for more refined approaches that delve into the design issues related to privacy, going beyond generic statements such as "the solution must respect privacy" and "organizations must consider privacy". To achieve this goal, the research team (*role*) conducted a thorough review of the existing literature on the IoT in occupational settings. The purpose of this review was to identify the key areas of privacy concern and associated risks that arise from the specific architecture of IoT in organizational contexts. We present the output of this review, along with supporting evidence, through six dimensions that pertain to data management and data flows (Shen et al. 2021):

Data collection within the IoT context entails the systematic acquisition of information from interconnected devices or sensors. This process, often conducted in real-time, aims to capture pertinent data points or events occurring within an organization's infrastructure or environment (Fabiano 2017b; Wang 2021). Consequently, the implementation of IoT technology in the workplace necessitates considering both online behaviors (e.g., screen time) and offline behaviors (e.g., location), which organizations must effectively manage. **Data processing** involves the transformation and analysis of the collected data. Computational techniques, algorithms, or statistical methods are employed to extract meaningful insights, patterns, or correlations (Shen et al. 2021; Wachter 2018b). The processed information facilitates informed decision-making or predictions for organizations. **Data storage** pertains to the structured retention and organization of the collected data by organizations, typically in databases or data repositories (Shen et al. 2021). **Data sharing** refers to the controlled dissemination or distribution of processed or raw data to authorized individuals, systems, or external entities. In the context of IoT, data sharing (as well as data storage) encompasses concepts such as property rights and data ownership (Perko 2022). In fact, these dimensions of data management are contingent upon **stakeholders** and **purpose**, as it is crucial to determine "with whom" the data will be shared and "for what purpose" (Perko 2022; Zhang et al. 2016). In IoT-driven OHS, various actors and stakeholders operate at different levels, impacting multiple groups with diverse interests and responsibilities (Negash et al. 2019). This includes organizations that adopt IoT technology, employees who receive real-time feedback on health and safety to enable preventive measures, and even third-party parties like data storage providers (e.g., LiquidWeb, Amazon, HIPAA Vault). Therefore, it is crucial to define the purpose of an IoT program, especially when handling sensitive data like health information (Häikiö et al. 2020; Naous and Mettler 2022). Organizations should aim to offer comprehensive information and streamline the objectives of the OHS initiative to minimize challenges associated with implementing innovation (Badii et al. 2019; Brous et al. 2020; Wei et al. 2011).

Activity 2: Insights from a Focus Group

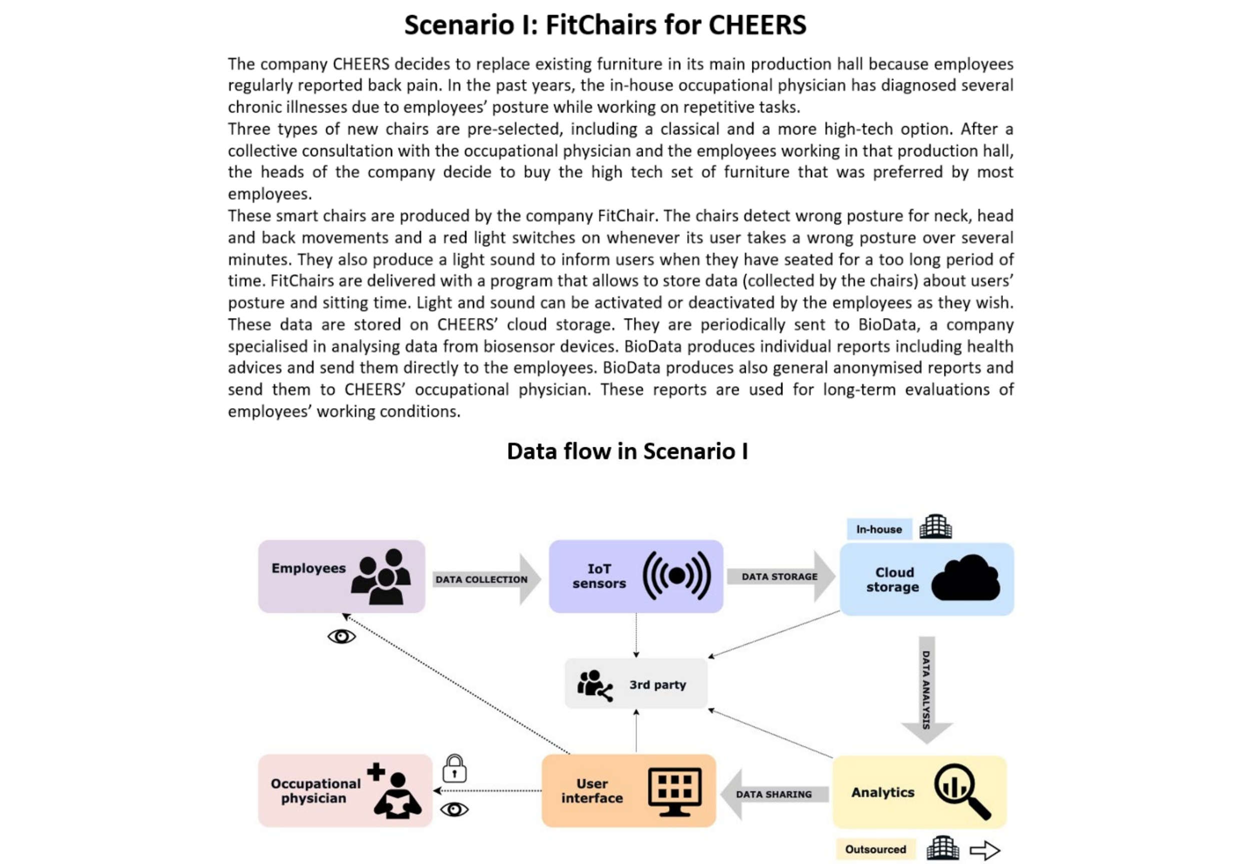
Technique: We organized a focus group with experts familiar with OHS (N=24) to gather insights on how organizations should assess privacy risks. Focus groups involve guiding participants through pre-determined topics and open-ended questions, enabling interactive discussions that incorporate individual insights and build upon each other's ideas (Sutton and Arnold 2013). This approach is valuable for extracting expertise and insights, especially in situations with limited data access or when studying new and emerging IS phenomena (O'hEocha et al. 2012; Sutton and Arnold 2013). The recruitment process aimed to achieve stakeholder diversity, including managers, employees, journalists, human resource members, researchers, and occupational health nurses, encompassing various demographic profiles. Recruitment methods involved personal recommendations and online searches instead of random sampling *(role: research team and expert panel*).

Three distinct scenarios were developed, each involving different elements such as connected chairs for improving posture, smart watches for promoting physical activity, and sound trackers for detecting stress. These scenarios varied in terms of device type, health focus, implementation duration, decision-making processes, activity scope, behavior recording, data storage, data analysis, and data accessibility. The focus group methodology, along with the utilization of scenarios, aligned with the dimensions mentioned in Activity 1. An illustration is shown in Figure 1, and all three scenarios can be viewed by using the following link: https://osf.io/vwb5k.

The focus group was recorded and transcribed, and the data was then anonymized. Verbatim segments were coded using *Atlas.ti* software. These codes were generated in a bottom-up approach and iteratively refined by the research team to classify emergent themes using word clouds and mind maps, resulting in a hierarchical structure of codes that were then paralleled with elements for Activity 1. Consistency checks were conducted by two of the authors and two other project members throughout the process to ensure alignment of codes, themes, and verbatim content. The main points derived from the analysis are as follows (output):

Firstly, regarding the **purpose of OHS**, our focus group experts emphasized the importance of organizations establishing clear boundaries between the use of IoT devices (and corresponding data) in the workplace and private settings. This precautionary measure is aimed to mitigate the risks associated with continuous monitoring and tracking of employees. Similarly, participants expressed the need for caution in aggregating and sharing data among organizations, as this has the potential to compromise individual privacy through comprehensive profiling and tracking. Therefore, in line with the insights provided by our experts, organizations should be mindful of the impact of increased surveillance and monitoring on employee autonomy, aiming to strike a balance that promotes safety without creating a hostile or oppressive atmosphere.

For our panel**, data collection** presented potential risks regarding the scope, volume, and type of data collected, ranging from research and statistical data to medical data. Participants suggested that data minimization should always be applied to enhance acceptability, regardless of data sensitivity.



Scenario I: FitChairs for CHEERS

The company CHEERS decides to replace existing furniture in its main production hall because employees regularly reported back pain. In the past years, the in-house occupational physician has diagnosed several chronic illnesses due to employees' posture while working on repetitive tasks.

Three types of new chairs are pre-selected, including a classical and a more high-tech option. After a collective consultation with the occupational physician and the employees working in that production hall, the heads of the company decide to buy the high tech set of furniture that was preferred by most employees.

These smart chairs are produced by the company FitChair. The chairs detect wrong posture for neck, head and back movements and a red light switches on whenever its user takes a wrong posture over several minutes. They also produce a light sound to inform users when they have seated for a too long period of time. FitChairs are delivered with a program that allows to store data (collected by the chairs) about users' posture and sitting time. Light and sound can be activated or deactivated by the employees as they wish. These data are stored on CHEERS' cloud storage. They are periodically sent to BioData, a company specialised in analysing data from biosensor devices. BioData produces individual reports including health advices and send them directly to the employees. BioData produces also general anonymised reports and send them to CHEERS' occupational physician. These reports are used for long-term evaluations of employees' working conditions.

Data flow in Scenario I

Figure 1. Example of a Fictive Scenario Used in the Focus Group

In the context of **data processing**, participants generally took a balanced view of internal and external analysis, including the involvement of third parties. This perspective was conditioned on the process being transparent and compliant, and on explicit user consent. Interestingly, third-party entities were often perceived as having superior analytical capabilities compared to internal resources, on the condition that they adhered to confidentiality principles. In fact, participants noted that internal resources often lack the necessary data processing expertise. Nevertheless, some participants considered internal processing to be more advantageous for gaining insight into employee particular needs, despite its potential drawbacks. Also, ensuring data quality during the processing stage was consistently highlighted as a critical issue by experts.

In terms of **data sharing** and **stakeholders**, discussions revolved around defining the boundaries of data access within organizations, particularly for departments such as IT and Human Resources. Externally, the consensus was that data should not be accessible to any third party without clear and explicit consent.

When it came to **data storage**, acceptance was higher when the solution was familiar and well-known. Outsourcing storage was considered acceptable under certain conditions, especially when the characteristics and terms of the outsourcing arrangement were clearly defined. Acceptance increased further when the outsourced storage solution was provided by a domestic actor.

Activity 3: Evidence from GDPR regulations and Academic Literature

Technique: We used a wide research string ("GDPR" OR "General Data Protection Regulation" AND "IoT" OR "Internet of Things") to gather a comprehensive range of studies. The research team (*role*) searched three key computer science and information technology databases: IEEE Xplore Digital Library, AIS

Electronic Library, and AISWorld (*tool*). These databases were selected based on their relevance to the IS discipline and their coverage of various topics (Schryen 2015). In addition, backward snowballing was employed to expand the scope by thoroughly searching the references until saturation (Wohlin 2014). The search was limited to English-language articles published between 2016 (GDPR came into force in May 2016 and is applicable from May 2018) and 2023, with a focus on GDPR and IoT. We used a narrative synthesis approach to identify privacy risks for organizations using IoT in the context of occupational health and safety (OHS), and structured them around identified GDPR principles (*output*). We had to adopt a rationale behind presenting the relationship between risks and GDPR principles, but it is important to note that these GDPR principles are all interconnected and interdependent.

Lawfulness, Fairness and Transparency

Transparency in purpose and data management information. In the context of IoT programs, the purpose of data collection should be clearly communicated to users, specifying the parties involved and the duration for which the data will be processed (Koutli et al. 2019).

Ensuring user consent. To comply with data protection regulations, organizations must obtain user consent. However, literature suggests that user consent for IoT in organizational settings often lacks quality (Ghayyur et al. 2020; Sengul 2017). This consent should be explicitly given through a statement (e.g., a signed consent) or clear affirmative action, allowing individuals to express their specific and informed wishes (Badii et al. 2020). Furthermore, the obtained consent should cover all processing activities carried out for the same purpose (Varadi et al. 2018).

Availability of opt-out options. Opt-out options allow users to stop data processing. This is typically aligned with the right to erasure, which involves the removal of all traces of data and the elimination of duplicate copies of data segments (Das et al. 2018; Sarkar et al. 2018; Wachter 2018b).

Purpose Limitation

Organizations should contain to the initial purpose of OHS. Organizations should strictly adhere to the initial purpose of OHS. Personal data should be collected for specified, explicit, and legitimate purposes and not be further processed in a way incompatible with those purposes. However, achieving this in Big Data scenarios can be challenging as, at the time of data collection, the purpose for future use may remain unclear (Forgó et al. 2017).

Organization should mitigate risks of profling. IoT and its various applications has the potential to generate user profiles. A significant repercussion of this is the possibility of users being erroneously classified or profiled into deceptive and misleading categories (Varkonyi et al. 2019).

Data Minimization

Limitation to necessary data in relation to initial purposes. Data processing should only involve the minimum amount of data necessary to successfully accomplish a given task. Failure to do so may result in excessive data collection (Kounoudes and Kapitsaki 2020).

Implementation of pseudonymization. Pseudonymization techniques, such as using nicknames, role pseudonyms, or relationship pseudonyms, have the potential to strengthen data privacy measures and mitigate associated risks (Badii et al. 2020).

Accuracy

Data can be updated and rectified where necessary. Specifically, Article 16 of the GDPR grants individuals the right to rectify their personal data if it is inaccurate or incomplete (Rhahla et al. 2019).

Data quality standards applied. Data quality standards hold significant importance in maintaining the accuracy of data. When low accuracy is attributed to a product or sensor, it can result in unreliable data that is not suitable for its intended use (Perez-Castillo et al. 2018). Consequently, the presence of unreliable or uncorrected information can have a detrimental impact on the interests of individuals involved.

Storage Limitation

Only necessary data storage during the duration of the project. With the IoT, vast amounts of data are continuously generated and stored, often without a clear understanding of the need for or duration of storage (Wachter 2018a). This poses significant risks to individual privacy, as unnecessary and prolonged data storage increases the potential for unauthorized access, data breaches, and misuse of personal information. To address these risks, organizations should ensure secure mechanisms for data storage, including consideration of responsible third-party involvement, type of storage (e.g., local or cloud), and access controls (Barati et al. 2020; Kounoudes and Kapitsaki 2020; Koutli et al. 2019) Additionally, data encryption can be employed to further safeguard data (Badii et al., 2020).

Integrity and Confidentiality

Certification and compliance to security standards. Organizations must implement robust security measures, including encryption, access controls, and regular monitoring, to protect IoT data and mitigate potential risks associated with the collection, processing, and storage of personal data (Alamri et al. 2021; Koutli et al. 2019; Rhahla et al. 2019). Furthermore, it is crucial for organizations to obtain certifications and furnish evidence of compliance, while concurrently establishing an effective security incident response management system to reinforce project support (Lee et al. 2019; Wachter 2018b).

Accountability

Identification of roles. Controllers and processors shall be able to demonstrate compliance with previous points. This involves implementing appropriate measures to ensure privacy and data protection, maintaining records of processing activities, and being able to demonstrate compliance upon request by regulatory authorities (Barati et al. 2019; Kounoudes and Kapitsaki 2020).

Activity 4: Method Compilation

Technique: The last activity corresponds to assembling our intermediary outputs (*Activities 1-3*) into a coherent (new) method (Ralyté et al. 2003). To do this, we created a comprehensive questionnaire that included all of the significant privacy risks identified in the previous activities (*see Table 2*). To ensure the validity of our questionnaire, we sought input from external experts who were not part of our research group. In addition, we converted the questionnaire into a website using PHP to have a cross-platform (mobile, web) entity that could be deployed on a public server.

Our questionnaire collects information related to the organizational scope and is designed to assist organizations in conducting a screening process. It serves to assess their compliance with regulations and guidelines, and even to evaluate their adherence to "community values". To streamline the assessment process, we developed a decision tree algorithm that relies primarily on binary responses ("yes" or "no") and assigns a value to each response. In cases where the responses indicate potential noncompliance with GDPR regulations (regarding the management of personal data), the questionnaire generates a report highlighting the specific principle and the area of noncompliance (see Figure 2).

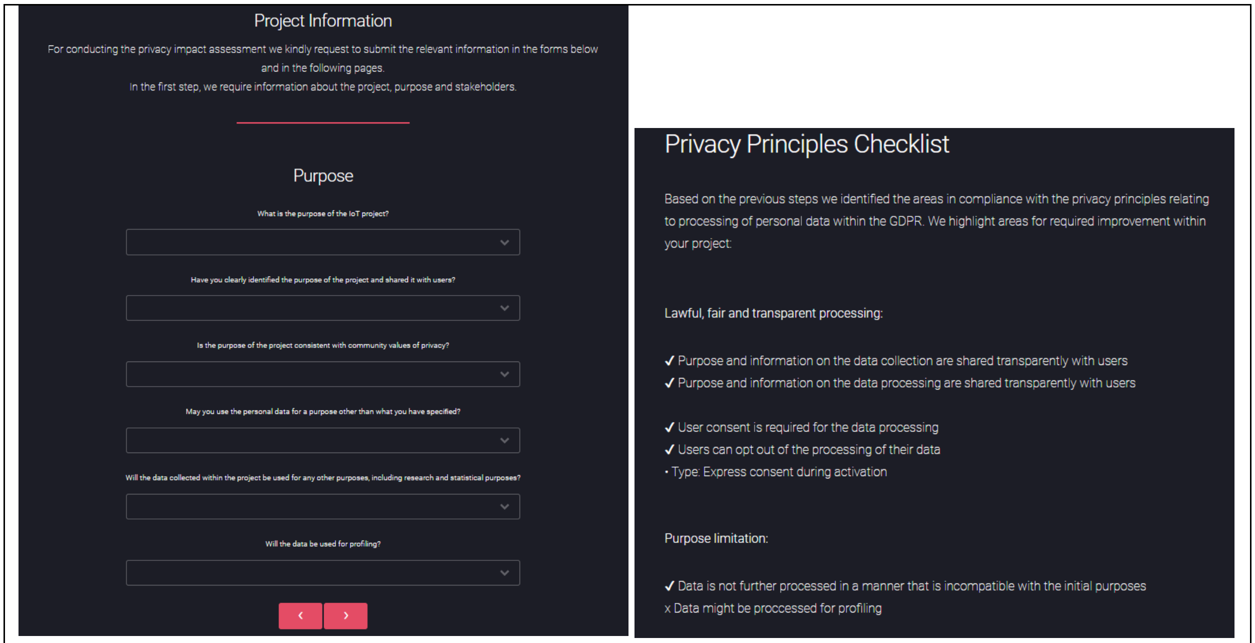
For example, when providing information about the purpose of a project, the following responses would result in a "non-compliant" score for the principle of processing data lawfully, fairly and transparently: "PUR2=No; PUR3=No; PUR5=Yes; PUR6=Yes". Similarly, for the principle of purpose limitation, the responses "PUR2=No; PUR3=No; PUR4=Yes; PUR6=Yes" would indicate noncompliance in this area.

Code	Questions	Answers
	Purpose	
PUR1	What is the purpose of the IoT project?	Physical health monitoring/ Emotional health monitoring/Environmental health monitoring/Other (please specify)
PUR2	Have you clearly identified the purpose of the project and shared it with users?	Yes/No
PUR3	Is the purpose of the project consistent with community values of privacy?	Yes/No
PUR4	May you use the personal data for a purpose other than what you have specified?	Yes/No
PUR5	Will the data collected within the project be used for any other purposes, including research and statistical purposes?	Yes/No
PUR6	Will the data be used for creating particular profiles of users?	Yes/No

Stakeholders		
STA1	Are the roles and responsibilities regarding data collection, data storage, data processing and data sharing defined?	Yes/No
Data sharing		
DSH1	Will all or part of the data management be executed by a third-party processor?	Yes/No
DSH2	Will all or part of the data be transferred to other organizations?	Yes/No
DSH3	Please specify if third party providers will be used at the following stages:	Data Collection/ Data Storage/ Data Processing
Data Collection		
DCO1	Does the project require the collection of sensitive data (such as personally identifiable data, biometric data, location data)?	Yes/No
DCO2	Will the data collected be combined with other data from outside the project?	Yes/No
DCO3	Can the data collected become personal due to linkage by third parties (such as phone number, location data, social ID, etc.)?	Yes/No
DCO4	Do the devices used rely on open-source technology?	Yes/No
DCO5	Is the user consent required for the collection of data?	Yes/No
DCO6	What type of consent is available for users?	Express consent during activation/Consent segmented per data category or processing type/ Express consent prior to sharing data
DCO7	Are users able to opt out of the collection or sharing of their information?	Yes/No
Data Storage		
DST1	Where will the data be stored?	Device manufacturer/Cloud solution/On-premise
DST2	If a cloud solution used, is the cloud provider compliant to security standards?	Yes/No
DST3	Does the user have the possibility to access his data?	Yes/No
DST4	Does the user have the possibility of retrieving personal data in order to transfer them to another service?	Yes/No
DST5	Does the user have the right to rectify personal data?	Yes/No
DST6	Does the user have the right to erase personal data?	Yes/No
DST7	Has the project taken measures to ensure protection of personal data (by means of encryption and/or access control)?	Yes/No
DST8	Have pseudonyms or codes been used to replace any data that could identify the individual?	Yes/No
DST9	What is the storage duration of the data collected?	No storage/1 year/3 years/Not determined
DST10	Has a system security plan (including data recovery) been completed for the information system(s) supporting the system?	Yes/No
Data Processing		
DPR1	Is there a possibility that data from various sources could be aggregated or matched in a way that undermines the person's anonymity?	Yes/No
DPR2	Has the project taken measures to ensure data quality?	Yes/No
DPR3	Do you have procedures in place to allow the subject individual to correct inaccurate or erroneous information?	Yes/No
DPR4	If data is transferred to third parties, is a detailed presentation of purposes of transmission provided to users?	Yes/No

Table 2. Questionnaire Used in the Privacy Impact Assessment (PIA) Method

From a technical standpoint, our PIA tool underwent evaluation by two independent engineers who specialize in GDPR compliance (respectively two and more than five years' experience in the field). The purpose of this evaluation was to ensure that the design, architecture, and functionalities of our website align with the best practices outlined in the GDPR. The assessment notability yield modifications of various privacy features, including CAPTCHA, user consent mechanisms, secure storage practices, and the incorporation of accessible options to contact members of our team.



Project Information

For conducting the privacy impact assessment we kindly request to submit the relevant information in the forms below and in the following pages.
In the first step, we require information about the project, purpose and stakeholders.

Purpose

What is the purpose of the IoT project?

Have you clearly identified the purpose of the project and shared it with users?

Is the purpose of the project consistent with community values of privacy?

May you use the personal data for a purpose other than what you have specified?

Will the data collected within the project be used for any other purposes, including research and statistical purposes?

Will the data be used for profiling?

Privacy Principles Checklist

Based on the previous steps we identified the areas in compliance with the privacy principles relating to processing of personal data within the GDPR. We highlight areas for required improvement within your project:

Lawful, fair and transparent processing:

✓ Purpose and information on the data collection are shared transparently with users
✓ Purpose and information on the data processing are shared transparently with users

✓ User consent is required for the data processing
✓ Users can opt out of the processing of their data
• Type: Express consent during activation

Purpose limitation:

✓ Data is not further processed in a manner that is incompatible with the initial purposes
x Data might be proccessed for profiling

Figure 2. Snapshots of the Privacy Impact Assessment (PIA) Tool

Discussion

The GDPR requires organizations using IoT devices to conduct privacy impact assessments (PIA), yet the GDPR lacks clarity in provisions relevant to IoT and PIAs. Existing recommendations tend to be vague and high-level, leading to subjective interpretations. This is problematic for OHS, where risk perception and privacy are crucial. Therefore, we propose to develop a tailored method and framework for conducting PIA in OHS. By doing so, we provide prescriptive knowledge to organizations, i.e. clear rules and instructions to help them objectively assess their GDPR compliance.

Our proposed method fulfills the basic attributes and elements of a method, as presented in Table 1. We provide a goal and strive to solve a concrete problem (i.e. helping organizations conduct privacy assessments). Through our design approach (SME), and through our design activities, we provide a set of instructions on how to achieve that goal (*systematic approach).* We also describe the specifications used to construct this method. Our method can be captured, reproduced, and tested for OHS programs (*reproducibility*) or serve as a foundation for other developments (e.g., PIAs for other IoT contexts).

In terms of method elements, our method clearly describes the tasks performed to obtain results at each step of the method development (*activity*). Similarly, the instructions outlining instructions to perform tasks (*technique*) are given, as well as the individuals involved (*role*), and the intermediate outputs. As a final production (or *output*), we propose the implementation of our method through a specialized tool, designed to support the application of the aforementioned techniques. The primary objective of this tool is to facilitate the utilization of our method by organizations seeking to evaluate the compliance of their OHS program with the regulations outlined in the GDPR.

Our PIA tool can typically assist smaller organizations that are in need of more concrete guidance and do not have the resources to navigate the vagueness of GPRD regulations. By utilizing our tool, these organizations can enhance their ability to implement GDPR requirements effectively. A PIA facilitates informed decision making by uncovering communication gaps and implicit assumptions within internal processes related to the project (Wright 2013). Additionally, it enables organizations to develop a deeper understanding of privacy-by-design principles and GDPR regulations. It is important to note that these GDPR principles are interconnected and should be applied collectively throughout the entire data management process. Consequently, organizations must adopt a comprehensive and ongoing approach to assess and review their data management practices to ensure compliance with these principles, as well as any supplementary obligations imposed by national laws and relevant regulatory bodies (Agyei and Oinas-Kukkonen 2020).

This change in philosophy can also be oriented towards data minimization. After a frantic race to collect as much data as possible (even if the relevance of collecting this data or its use is unclear), organizations are now urged to exercise restraint in order to avoid complications with users and regulatory frameworks (Fabiano 2017a). Cavoukian and Chibba (2009) have highlighted the necessity to embrace a "design thinking" approach to foster innovation, creativity, and competitiveness. This approach involves a comprehensive, interdisciplinary, and integrative perspective that facilitates the identification and resolution of constraints. Similarly, privacy concerns should be addressed through the lens of design thinking, where privacy becomes an intrinsic characteristic of networked data systems and technologies, established as the default configuration (Oetzel and Spiekermann 2014).

In the same line, we present a detailed description of the methodology used in our PIA tool. Our goal is to contribute to the standardization and documentation required for the use of new and emerging technologies. This effort is particularly important in the early stages of design and pre-processing, as it addresses the growing need for unfairness and bias mitigation (Galdon Clavell et al. 2020). This approach aligns with existing literature that recognizes the challenges facing industry experts, who often lack sufficient resources to effectively address some risk or bias issues in IoT contexts (Krieg et al. 2017). In order to mitigate potential prejudice before a system is implemented, the collection of interaction records can assist auditors of algorithms. Therefore, advocating for ongoing documentation of models is essential as it allows for the auditing of IoT ultimately reducing the influence of privacy risks.

In addition, our PIA serves to build trust between organizations and individuals by demonstrating a commitment to privacy and data protection. Transparency regarding data processing practices and involving individuals in the assessment process are critical to fostering trust among stakeholders (Horák et al. 2019; Perez-Castillo et al. 2018). An illustrative instance of this can be observed in the context of a healthcare organization employing IoT devices for remote patient monitoring. Undertaking a PIA becomes indispensable in this scenario, as it serves to instill faith in the system by providing privacy protections and promoting transparency (Elkhodr et al. 2019).

Finally, our approach serves to provide a contextualized framework for evaluating privacy in the context of IoT. Defining a clear context for the use of IoT and establishing a clear user-controlled disclosure of personal data helps to prevent the risk of profiling and collection of characteristics that may affect the privacy of users. It serves also to inform individuals about the risks of profiling at the earliest possible stage so that they can exercise their rights (Bietti 2020).

Still, the limitations of PIAs and their effectiveness in addressing user awareness and control over personal data need to be examined. When evaluating technical and organizational measures, PIAs may not adequately consider users' ability to understand and manage their privacy settings (Oetzel and Spiekermann 2014; Wachter 2018a). This limitation may impede users' ability to exercise control over their personal data within IoT systems.

The importance of conducting a PIA can be diminished when the interests of companies are threatened by positive policy changes. This challenge is particularly evident in areas such as big data, where there is a constant tension between systemic concerns about fundamental rights and companies' pursuit of normalizing practices and maximizing profits (Bietti 2020). As long as the final decision-making authority on IoT remains with the company itself, internal ethics programs will primarily serve the interests of the company rather than those of users and society at large. As a result, these programs may lack significant practical value in a comprehensive assessment.

In addition, PIAs often focus on specific points in time and may not fully capture emerging privacy risks associated with rapidly evolving technologies. Ex-ante or ex-post risk assessments are often based on overly simplistic assumptions that risks can always be accurately predicted (Ahmadian et al. 2018). The uncertainty lies in our inability to definitively predict how technologies will be used in the future (i.e., unintended use), making it highly unlikely that risk assessment methods can accurately estimate the full risk of technologies. Who could have predicted that social media platforms would be used for political influence, regime change, and the spread of disinformation? Even the most robust methodologies cannot predict such unforeseen events, often referred to as "black swans".

In sum, PIAs must be considered in their own particular environments. Likewise, the relevance of the results of their assessment must be balanced against the actual context. As Vemou and Karyda (2018) point out, there is a risk of providing outdated technical controls due to the rapid advancement of technology, which can mislead PIA practitioners who rely solely on provided control lists.

Limitations and Future Work

The primary focus of our paper has been on the construction of the underlying model of our PIA tool. However, there is room for further refinement of our tool, particularly by incorporating various developments to enhance its practical value. One critical aspect that needs to be addressed is the necessity of a more didactic interface. This may help to provide more comprehensive explanations and guidance throughout the assessment process. Also, by incorporating additional visualization tools, we can improve user-friendliness and facilitate rapid understanding of potential risks.

While our current report provides an overview of compliance and highlights areas of privacy risk, it does not generate specific recommendations for organizations. At a more advanced stage, our tool could be enhanced to provide risk scores and quantitative impact assessments. This would help assess the level of risk associated with GDPR, quantify potential harm to users, and even conduct ethical assessments (Wagner and Boiten 2018). Moreover, PIAs focus primarily on the right to privacy, which is the individual facet of data protection. However, they may not cover ethical and societal concerns (e.g. justice, social solidarity, etc.) that may affect fundamental rights and freedoms (Mantelero 2018; Yam and Skorburg 2021). Therefore, organizations, particularly project managers overseeing a project, should consider the environmental, social, and organizational contexts to strengthen the PIA's ability to adequately protect individuals' privacy rights and overall well-being.

Similarly, to ensure the robustness of the tool's operationalization, it is essential to refine it through testing with real use cases (Saunders and Jones 1992). Likewise, the method itself may need to be modified. PIAs require ongoing refinement and reassessment to address potential gaps in the methodology and to keep pace with evolving privacy needs and regulatory developments (Oetzel and Spiekermann 2014; Wright 2013).

In conclusion, our research highlights the importance of PIAs as a critical component within comprehensive privacy management frameworks. Our study presents a PIA method and a PIA tool specifically designed to provide organizations with an objective means of assessing the privacy risks associated with IoT projects in the workplace. By using this approach, organizations can make informed decisions about integrating IoT initiatives while considering the potential privacy implications.

It is important to recognize that the effectiveness of the PIA depends on the organization's commitment to privacy. However, we believe that by adopting our approach, organizations can foster a culture of responsibility and ethics in the handling of personal data. This approach allows organizations to capitalize on the valuable insights that IoT projects provide, while ensuring that individuals' privacy rights are protected.

Acknowledgements

This research has been conducted within the Swiss National Research Programme (NRP77) on “Digital Transformation” and received funding from the Swiss National Science Foundation (grant no. 187429).

References

Aanestad, M., Mähring, M., Østerlund, C., Riemer, K., and Schultze, U. 2018. "Living with Monsters?," *Living with Monsters? Social Implications of Algorithmic Phenomena, Hybrid Agency, and the Performativity of Technology: IFIP WG 8.2 Working Conference on the Interaction of Information Systems and the Organization, IS&O 2018, San Francisco, CA, USA, December 11-12, 2018, Proceedings*: Springer, pp. 3-12.

Agyei, E. E. Y. F., and Oinas-Kukkonen, H. 2020. "Gdpr and Systems for Health Behavior Change: A Systematic Review," *Persuasive Technology. Designing for Future Change: 15th International Conference on Persuasive Technology, PERSUASIVE 2020, Aalborg, Denmark, April 20–23, 2020, Proceedings 15*: Springer, pp. 234-246.

Ahmadian, A. S., Strüber, D., Riediger, V., and Jürjens, J. 2018. "Supporting Privacy Impact Assessment by Model-Based Privacy Analysis," *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, pp. 1467-1474.

Ailneni, R. C., Syamala, K. R., Kim, I.-S., and Hwang, J. 2019. "Influence of the Wearable Posture Correction Sensor on Head and Neck Posture: Sitting and Standing Workstations," *Work* (62:1), pp. 27-35.

Akhlaghpour, S., Hassandoust, F., Fatehi, F., Burton-Jones, A., and Hynd, A. 2021. "Learning from Enforcement Cases to Manage Gdpr Risks," *MIS Quarterly Executive* (20:3), pp. 199-218.

Akil, M., Islami, L., Fischer-Hübner, S., Martucci, L. A., and Zuccato, A. 2020. "Privacy-Preserving Identifiers for Iot: A Systematic Literature Review," *IEEE Access* (8), pp. 168470-168485.

Alamri, B., Javed, I. T., and Margaria, T. 2021. "A Gdpr-Compliant Framework for Iot-Based Personal Health Records Using Blockchain," *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1-5.

Asadi, M., and Ramsin, R. 2009. "Patterns of Situational Method Engineering," *Software Engineering Research, Management and Applications 2009*), pp. 277-291.

Badii, C., Bellini, P., Cenni, D., Mitolo, N., Nesi, P., Pantaleo, G., and Soderi, M. 2020. "Industry 4.0 Synoptics Controlled by Iot Applications in Node-Red," *2020 International Conferences on Internet of Things (iThings)*, pp. 54-61.

Badii, C., Bellini, P., Difino, A., and Nesi, P. 2019. "Privacy and Security Aspects on a Smart City Iot Platform," *2019 IEEE SmartWorld, ,* pp. 1371-1376.

Barati, M., Petri, I., and Rana, O. F. 2019. "Developing Gdpr Compliant User Data Policies for Internet of Things," in: *Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing*. Auckland, New Zealand: Association for Computing Machinery, pp. 133–141.

Barati, M., Rana, O., Petri, I., and Theodorakopoulos, G. 2020. "Gdpr Compliance Verification in Internet of Things," *IEEE Access* (8), pp. 119697-119709.

Bietti, E. 2020. "From Ethics Washing to Ethics Bashing: A View on Tech Ethics from within Moral Philosophy," *Proceedings of the 2020 conference on fairness, accountability, and transparency*, pp. 210-219.

Braun, C., Wortmann, F., Hafner, M., and Winter, R. 2005. "Method Construction-a Core Approach to Organizational Engineering," *Proceedings of the 2005 ACM symposium on Applied computing*, pp. 1295-1299.

Brous, P., Janssen, M., and Herder, P. 2020. "The Dual Effects of the Internet of Things (Iot): A Systematic Review of the Benefits and Risks of Iot Adoption by Organizations," *International Journal of Information Management* (51), p. 101952.

Castelluccia, C., Cunche, M., Metayer, D. L., and Morel, V. 2018. "Enhancing Transparency and Consent in the Iot," *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 116-119.

Cavoukian, A., and Chibba, M. 2009. "Advancing Privacy and Security in Computing, Networking and Systems Innovations through Privacy by Design," *Proceedings of the 2009 Conference of the Center for Advanced Studies on Collaborative Research*, pp. 358-360.

Clarke, R. 2009. "Privacy Impact Assessment: Its Origins and Development," *Computer law & security review* (25:2), pp. 123-135.

Das, A., Degeling, M., Smullen, D., and Sadeh, N. 2018. "Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice," *IEEE Pervasive Computing* (17:3), pp. 35-46.

Denner, M.-S., Püschel, L. C., and Röglinger, M. 2018. "How to Exploit the Digitalization Potential of Business Processes," *Business & Information Systems Engineering* (60), pp. 331-349.

Elkhodr, M., Alsinglawi, B., and Alshehri, M. 2019. "A Privacy Risk Assessment for the Internet of Things in Healthcare," *Applications of intelligent technologies in healthcare*), pp. 47-54.

Fabiano, N. 2017a. "Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard," *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 727-734.

Fabiano, N. 2017b. "The Internet of Things Ecosystem: The Blockchain and Privacy Issues. The Challenge for a Global Privacy Standard," *2017 International Conference on Internet of Things for the Global Community (IoTGC)*, pp. 1-7.

Forgó, N., Hänold, S., and Schütze, B. 2017. "The Principle of Purpose Limitation and Big Data," *New technology, big data and the law*), pp. 17-42.

Fridgen, G., Lockl, J., Radszuwill, S., Rieger, A., Schweizer, A., and Urbach, N. 2018. "A Solution in Search of a Problem: A Method for the Development of Blockchain Use Cases," *AMCIS*, pp. 1-11.

Galdon Clavell, G., Martín Zamorano, M., Castillo, C., Smith, O., and Matic, A. 2020. "Auditing Algorithms: On Lessons Learned and the Risks of Data Minimization," *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, pp. 265-271.

Ghayyur, S., Pappachan, P., Wang, G., Mehrotra, S., and Venkatasubramanian, N. 2020. "Designing Privacy Preserving Data Sharing Middleware for Internet of Things," in: *Proceedings of the Third Workshop on Data: Acquisition To Analysis*. Virtual Event, Japan: Association for Computing Machinery, pp. 1–6.

Glance, D. G., Ooi, E., Berman, Y. e., Glance, C. F., and Barrett, H. R. 2016. "Impact of a Digital Activity Tracker-Based Workplace Activity Program on Health and Wellbeing," *Proceedings of the 6th International Conference on Digital Health Conference*, Montreal, Canada, pp. 37-41.

Golightly, L., Wnuk, K., Shanmugan, N., Shaban, A., Longstaff, J., and Chang, V. 2022. "Towards a Working Conceptual Framework: Cyber Law for Data Privacy and Information Security Management for the Industrial Internet of Things Application Domain," *2022 International Conference on Industrial IoT, Big Data and Supply Chain (IIoTBDSC)*, pp. 86-94.

Gonzalez-Granadillo, G., Menesidou, S. A., Papamartzivanos, D., Romeu, R., Navarro-Llobet, D., Okoh, C., Nifakos, S., Xenakis, C., and Panaousis, E. 2021. "Automated Cyber and Privacy Risk Management Toolkit," *Sensors* (21:16), pp. 1-28.

Gonzalez-Perez, C., Giorgini, P., and Henderson-Sellers, B. 2009. "Method Construction by Goal Analysis," *Information Systems Development: Challenges in Practice, Theory, and Education Volume 1*), pp. 79-91.

Häikiö, J., Kallio, J., Mäkelä, S.-M., and Keränen, J. 2020. "Iot-Based Safety Monitoring from the Perspective of Construction Site Workers," *International Journal of Occupational and Environmental Safety* (4:1), pp. 1-14.

Horák, M., Stupka, V., and Husák, M. 2019. "Gdpr Compliance in Cybersecurity Software: A Case Study of Dpia in Information Sharing Platform," *Proceedings of the 14th international conference on availability, reliability and security*, pp. 1-8.

Khan, W. Z., Aalsalem, M. Y., Khan, M. K., and Arshad, Q. 2016. "Enabling Consumer Trust Upon Acceptance of Iot Technologies through Security and Privacy Model," *Advanced Multimedia and Ubiquitous Engineering: FutureTech & MUE*: Springer, pp. 111-117.

Kounoudes, A. D., and Kapitsaki, G. M. 2020. "A Mapping of Iot User-Centric Privacy Preserving Approaches to the Gdpr," *Internet of Things* (11), p. 100179.

Koutli, M., Theologou, N., Tryferidis, A., Tzovaras, D., Kagkini, A., Zandes, D., Karkaletsis, K., Kaggelides, K., Miralles, J. A., Oravec, V., and Vanya, S. 2019. "Secure Iot E-Health Applications Using Vicinity Framework and Gdpr Guidelines," *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 263-270.

Krieg, L. J., Berning, M., and Hardon, A. 2017. "Anthropology with Algorithms?," *Medicine Anthropology Theory* (4:3), pp. 21-52.

Lee, G. Y., Cha, K. J., and Kim, H. J. 2019. "Designing the Gdpr Compliant Consent Procedure for Personal Information Collection in the Iot Environment," *2019 IEEE International Congress on Internet of Things (ICIOT)*, pp. 79-81.

Lupton, D., and Michael, M. 2017. "'Depends on Who's Got the Data': Public Understandings of Personal Digital Dataveillance," *Surveillance & Society* (15:2), pp. 254-268.

Mantelero, A. 2018. "Ai and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment," *Computer Law & Security Review* (34:4), pp. 754-772.

March, S. T., and Smith, G. F. 1995. "Design and Natural Science Research on Information Technology," *Decision support systems* (15:4), pp. 251-266.

Mettler, T., and Naous, D. 2022. "Beyond Panoptic Surveillance: On the Ethical Dilemmas of the Connected Workplace," *Proceedings of the Thirtieth European Conference on Information Systems*, Timisoara, Romania, pp. 1-16.

Mettler, T., and Wulf, J. 2019. "Physiolytics at the Workplace: Affordances and Constraints of Wearables Use from an Employee's Perspective," *Information Systems Journal* (29:1), pp. 1-29.

Naous, D., and Mettler, T. 2022. "Mental Health Monitoring at Work: Iot Solutions and Privacy Concerns," *Well-Being in the Information Society: When the Mind Breaks: 9th International Conference, WIS 2022, Turku, Finland, August 25–26, 2022, Proceedings*: Springer, pp. 37-45.

Negash, B., Westerlund, T., and Tenhunen, H. 2019. "Towards an Interoperable Internet of Things through a Web of Virtual Things at the Fog Layer," *Future Generation Computer Systems* (91), pp. 96-107.

Nižetić, S., Pivac, N., Zanki, V., and Papadopoulos, A. M. 2020. "Application of Smart Wearable Sensors in Office Buildings for Modelling of Occupants' Metabolic Responses," *Energy and Buildings* (226), p. 110399.

O'hEocha, C., Wang, X., and Conboy, K. 2012. "The Use of Focus Groups in Complex and Pressurised Is Studies and Evaluation Using Klein & Myers Principles for Interpretive Research," *Information Systems Journal* (22:3), pp. 235-256.

Oetzel, M. C., and Spiekermann, S. 2014. "A Systematic Methodology for Privacy Impact Assessments: A Design Science Approach," *European Journal of Information Systems* (23:2), pp. 126-150.

Perez-Castillo, R., Carretero, A. G., Rodriguez, M., Caballero, I., Piattini, M., Mate, A., Kim, S., and Lee, D. 2018. "Data Quality Best Practices in Iot Environments," *2018 11th International Conference on the Quality of Information and Communications Technology (QUATIC)*: IEEE, pp. 272-275.

Perko, I. 2022. "Data Sharing Concepts: A Viable System Model Diagnosis," *Kybernetes*:ahead-of-print), pp. 1-16.

Psychoula, I., Singh, D., Chen, L., Chen, F., Holzinger, A., and Ning, H. 2018. "Users' Privacy Concerns in Iot Based Applications," *2018 IEEE SmartWorld*: IEEE, pp. 1887-1894.

Ralyté, J., Deneckère, R., and Rolland, C. 2003. "Towards a Generic Model for Situational Method Engineering," *Advanced Information Systems Engineering: 15th International Conference, CAiSE 2003 Klagenfurt/Velden, Austria, June 16–20, 2003 Proceedings 15*: Springer, pp. 95-110.

Regulation, P. 2016. "Regulation (Eu) 2016/679 of the European Parliament and of the Council," *Regulation (eu)* (679), p. 2016.

Rhahla, M., Abdellatif, T., Attia, R., and Berrayana, W. 2019. "A Gdpr Controller for Iot Systems: Application to E-Health," *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, pp. 170-173.

Rolland, C., and Prakash, N. 1996. "A Proposal for Context-Specific Method Engineering," *Method engineering: Principles of method construction and tool support*), pp. 191-208.

Roossien, C., Stegenga, J., Hodselmans, A., Spook, S., Koolhaas, W., Brouwer, S., Verkerke, G., and Reneman, M. F. 2017. "Can a Smart Chair Improve the Sitting Behavior of Office Workers?," *Applied ergonomics* (65), pp. 355-361.

Sarkar, S., Banatre, J. P., Rilling, L., and Morin, C. 2018. "Towards Enforcement of the Eu Gdpr: Enabling Data Erasure," *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 222-229.

Saunders, C. S., and Jones, J. W. 1992. "Measuring Performance of the Information Systems Function," *Journal of Management Information Systems* (8:4), pp. 63-82.

Schryen, G. 2015. "Writing Qualitative Is Literature Reviews—Guidelines for Synthesis, Interpretation, and Guidance of Research," *Communications of the Association for Information Systems* (37:1), p. 12.

Sengul, C. 2017. "Privacy, Consent and Authorization in Iot," *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*, pp. 319-321.

Shen, X. S., Huang, C., Liu, D., Xue, L., Zhuang, W., Sun, R., and Ying, B. 2021. "Data Management for Future Wireless Networks: Architecture, Privacy Preservation, and Regulation," *IEEE Network* (35:1), pp. 8-15.

Stepanovic, S., Mozgovoy, V., and Mettler, T. 2019. "Designing Visualizations for Workplace Stress Management: Results of a Pilot Study at a Swiss Municipality," in *International Conference on Electronic Government*. Berlin: Springer, pp. 94-104.

Stephenson, A., McDonough, S. M., Murphy, M. H., Nugent, C. D., and Mair, J. L. 2017. "Using Computer, Mobile and Wearable Technology Enhanced Interventions to Reduce Sedentary Behaviour: A Systematic Review and Meta-Analysis," *International Journal of Behavioral Nutrition and Physical Activity* (14:1), p. 105.

Sutton, S. G., and Arnold, V. 2013. "Focus Group Methods: Using Interactive and Nominal Groups to Explore Emerging Technology-Driven Phenomena in Accounting and Information Systems," *International Journal of Accounting Information Systems* (14:2), pp. 81-88.

Synnott, J., Rafferty, J., and Nugent, C. D. 2016. "Detection of Workplace Sedentary Behavior Using Thermal Sensors," *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*: IEEE, pp. 5413-5416.

Tancock, D., Pearson, S., and Charlesworth, A. 2013. "A Privacy Impact Assessment Tool for Cloud Computing," *Privacy and security for Cloud computing*), pp. 73-123.

Tawalbeh, L. a., Muheidat, F., Tawalbeh, M., and Quwaider, M. 2020. "Iot Privacy and Security: Challenges and Solutions," *Applied Sciences* (10:12 - 4102), pp. 1-17.

Varadi, S., Varkonyi, G. G., and Kertesz, A. 2018. "Law and Iot: How to See Things Clearly in the Fog," *2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)*, pp. 233-238.

Varkonyi, G. G., Kertesz, A., and Varadi, S. 2019. "Privacy-Awareness of Users in Our Cloudy Smart World," *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*, pp. 189-196.

Vegh, L. 2018. "A Survey of Privacy and Security Issues for the Internet of Things in the Gdpr Era," *2018 International Conference on Communications (COMM)*, pp. 453-458.

Vemou, K., and Karyda, M. 2018. "An Evaluation Framework for Privacy Impact Assessment Methods," *Mediterranean Conference on Information Systems (MCIS)*, Corfou, Greece, pp. 1-11.

Venkatesh, D. A. N. 2017. "Connecting the Dots: Internet of Things and Human Resource Management," *American International Journal of Research in Humanities, Arts and Social Sciences, ISSN (Print)*), pp. 2328-3734.

Wachter, S. 2018a. "Ethical and Normative Challenges of Identification in the Internet of Things," *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, pp. 1-10.

Wachter, S. 2018b. "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the Gdpr," *Computer law & security review* (34:3), pp. 436-449.

Wagner, I., and Boiten, E. 2018. "Privacy Risk Assessment: From Art to Science, by Metrics," *Data Privacy Management, Cryptocurrencies and Blockchain Technology*,, Barcelona, Spain: Springer, pp. 225-241.

Wang, G. 2021. "Phd Forum Abstract: Privacy-Preserving Data Collection and Sharing in Smart Spaces," *2021 IEEE International Conference on Smart Computing (SMARTCOMP)*, pp. 416-417.

Warren, A., Bayley, R., Bennett, C., Charlesworth, A., Clarke, R., and Oppenheim, C. 2008. "Privacy Impact Assessments: International Experience as a Basis for Uk Guidance," *Computer Law & Security Review* (24:3), pp. 233-242.

Wei, K.-K., Teo, H.-H., Chan, H. C., and Tan, B. C. 2011. "Conceptualizing and Testing a Social Cognitive Model of the Digital Divide," *Information Systems Research* (22:1), pp. 170-187.

Wohlin, C. 2014. "Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering," *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, London, England, United Kingdom: ACM, pp. 1-10.

Wright, D. 2013. "Making Privacy Impact Assessment More Effective," *The Information Society* (29:5), pp. 307-315.

Yam, J., and Skorburg, J. A. 2021. "From Human Resources to Human Rights: Impact Assessments for Hiring Algorithms," *Ethics and Information Technology* (23:4), pp. 611-623.

Yassaee, M., and Mettler, T. 2017. "Digital Occupational Health Systems: What Do Employees Think About It?," *Information Systems Frontiers* (19:8), pp. 1-16.

Zhang, Q., Zhang, X., Zhang, Q., Shi, W., and Zhong, H. 2016. "Firework: Big Data Sharing and Processing in Collaborative Edge Environment," *2016 Fourth IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*: IEEE, pp. 20-25.