A Framework to Navigate the Privacy Trade-offs for Human-Centred Manufacturing

Sobah Abbas Petersen, Felix Mannhardt, Manuel Oliveira, Hans Torvatn

A Framework to Navigate the Privacy Trade-offs for Human-Centred Manufacturing

Sobah Abbas Petersen, Felix Mannhardt, Manuel Oliveira, Hans Torvatn

SINTEF Technology and Society, Trondheim, Norway
{Sobah.Petersen, Felix.Mannhardt, Manuel.Oliveira, Hans.Torvatn}@sintef.no

Abstract. New technological advances can offer personalised and timely services for industry workers. Exoskeletons, HoloLens, Process Mining and Social Knowledge Networks are some of these services offered to workers by the EU HuMan project. These services could alleviate a worker's physical stress, their cognitive load or provide help based on the knowledge and experiences of their peers. The successful application of several such services depends on the availability of data about a worker's state, including their performance. This paper focusses on the design of cognitive systems that provide personalied services while respecting a worker's privacy and the needs of an organisation. We present a framework for supporting privacy by design and the risks, threats and needs of users, organisations and developers.

Keywords: Privacy, Trust, Manufacturing, Real-time support, Human Centred

1 Introduction

Privacy has been defined as "the right to be left alone" [1]. It is a concept that has sparked many discussions in several domains. In 1890, Warren and Brandeis wrote an article in the Harvard Law Review, which was one of the most influential essays in the history of American Law. Privacy was considered from the perspective of a human being, e.g. if they are pursued, bothered or harmed by others. A broader perspective of affecting a human being beyond physical harm was also considered, such as if their feelings were affected or someone's private life was invaded. As we are well aware, these continue to be concerns of privacy even today.

The focus of privacy has been on the protection of data pertaining to a person; i.e. protection of personal information with an emphasis on data security and methods, frameworks and techniques for ensuring appropriate data security. However, in the age of ubiquitous computing and social networks, such a data-centric view that disregards the influence of human factors is inadequate and the need for a more person-centric view of privacy is required, e.g. [2]. In fact, with increasing accessibility to data and the technology to aggregate data and conduct sophisticated analyses at workplaces, the need to protect the data and the privacy of individuals is more important than ever before. The area of Human Factors and Ergonomics (HFE) has focused on safety and security at the workplace, part of which is also data security; e.g. [3].

In Industry 4.0, the use of smart technologies and sensors are seen as the future of manufacturing [4]. Tomorrow's factories [5] will leverage on new and emerging technologies and digital solutions to enhance collaboration not only among the workers, but also between the human workers and technology – Human in the Loop (HITL). Technologies such as exoskeletons and other wearables promise collaboration networks between humans and technology, leading to improved health and safety at the workplace [6] and reduced physiological load. Combined with sophisticated analytics and insights, cognitive systems are developed to provide timely and relevant support to workers. Similarly, other types of technologies, such as Augmented Reality, support workers with cognitive load minimisation and performance improvement [7]. Collaborative and cognitive networks include different types of technologies, such as social and cognitive assistive technologies, enhanced data collection and potential risks for privacy and data security [3].

The attention to the privacy protection of individuals at their workplaces or in society has been a priority of many countries, the most recent of which is the European Union's General Data Protection Regulation (GDPR). GDPR defines personal data as ”any information relating to an identified or identifiable natural person (data subject)”. Methods such as data anonymisation or pseudonymising needs rethinking, to ensure that personal data is processed with the aim to irreversibly prevent the identification of the individual to whom the data relates to. The GDPR provides new rights to the data subjects where they now have control of their data, improving data transparency and empowerment of data subjects [11]. It focuses on the protection of personal data and not only on the privacy of personal data, increasing the need to be clear about who has access to data and how data is used. To achieve this, it is also important that the data provider trusts the data receiver to not misuse the data. Data privacy, thus, goes beyond technological solutions into the softer aspects of an organisation, such as the individual’s trust in the organisation in the use of the collated data. This would mean that trusting employees would give their consent to the organisation to collect, store and process their personal data [12]. Consciously working to deliver value in exchange for personal data that is collected and highlighting and communicating the benefits to the employees can foster trust.

The introduction of GDPR raises awareness among employees, organisations and technology developers on protecting employees by protecting their personal data. At the same time, we have become used to the personalised services that are on offer, such as the personalised recommendations through online systems, often oblivious to the fact that it is the personal data collected through our digital footprint that has facilitated such services. This inconsistency between privacy attitudes and privacy behaviour of individuals is coined the privacy paradox [8].

The aim of this paper is to draw attention to the privacy concerns of operators in the manufacturing industry and support developers of technologies to adopt privacy by design as their default practice. The main research focus is on the revelations about GDPR concerns and identifying the risks, threats, and needs perceived by users and developers when dealing with the privacy-personalisation trade-offs in cognitive systems. We do this by presenting a framework for Trust and Privacy design, developed within the context of the EU H2020 HuMan [10] project. The main research activities that contributed to the HuMan Trust and Privacy Framework (TPF) were a literature review of Privacy and Trust models, a workshop with the use case partners in the HuMan project and the analysis of GDPR. The HuMan TPF was then presented to the project consortium and a second workshop was held with the end-user companies and the technology developers. This paper reports the outcomes of both these workshops from the two perspectives of both the users and the developers.

This paper is structured as follows: Section 2 describes the HuMan project and some of the HuMan services; Section 3; describes the HuMan TPF; Section 4 presents and overview of the users' perspectives; Section 5 provides an overview of the developers' perspectives; Section 6 presents the feedback on the framework and finally Section 7 summarises the paper.

2. HuMAN Project

The EU H2020 HuMAN project aims to digitally enhance the operator on the shopfloor to support them in their work, assisting them in mitigating any productivity losses resulting from both physical and cognitive fatigue whilst contributing to greater well-being. Towards this goal, the cognitive system envisioned in HuMan captures physiological data from the operator (through wearable sensors), is aware of the production context (e.g. tasks, workplace) in which the operator is embedded and uses data analytics on historical data to provide timely and contextualised support for operators. The HuMan cognitive system monitors these data streams and is able to determine when an intervention is needed, for example, due to an increased stress level that was detected for an operator. The HuMan system is organised as several loosely coupled services that exchange and consume data through a shared middleware (event bus) provided by the HuMan core solution. The data that is exchanged may be used directly in a real-time fashion or is stored for later analysis. An example for the direct usage of data is the automatic detection of whether there is need for an intervention. An example for indirect usage is the improvement of work places or work processes by analysing aggregated historical data. Some of the services that are developed in the HuMan project are Exoskeleton (EXOS), Shopfloor Insight Intelligence (SII) and Social Knowledge Network (SKN).

The EXOS service is coupled to a light-weight exoskeleton that an operator wears to distribute the physical stress on their body, reducing the likelihood of injury and allowing the operator to maintain their optimal performance levels. The HuMan solution monitors the different physiological signals, such as heart rate and galvanic skin response, to determine the onset of fatigue and thereby activate the exoskeleton. The service then adjusts the level of support in proportion to the level of physical stress until operational parameters have exceeded and the operator is advised to take a rest, as the device is unable to further assist them. EXOS monitors physiological data which may be correlated to the operator’s performance to provide real-time support.

The SKN service leverages on the collective knowledge and experience of peers by using ideas from social computing and captures and stores media directly related to an operator’s activity. In addition, the level of engagement and how the operator contributes to the curation of knowledge can be assessed. The SKN service uses stored data, particularly captured via Social Networks.

The SII is one of the data analytics component of the HuMan system and relies on the captured data from other services. It combines data from several sources into a coherent event log and applies process mining methods to reveal what actually happened on the shop-floor [13]. Based on aggregated data as well as individual executions of work processes, the SII aims to reveal and help identifying root causes for recurring physical and cognitive stress that cannot be alleviated automatically by the available intervention measures of the HuMan system.

3 HuMan Privacy and Trust Framework

In the HuMan project, we have developed a Trust and Privacy Framework to increase awareness of privacy and trust issues among individuals and to support developers in achieving privacy by design. Several models of Privacy in the literature emphasise the relevance of the flow of information or data (e.g. [14], [15]), the use information or data (e.g. [16], [17]) and the visibility or who has access to personal data (e.g. [18]). Trust models from literature draw attention to the role of the "trustor" and "trustee" and the interaction between them [19], and how trust may be learned or built over time or from situational cues [20]. Dimensions of trust identified in the literature include the trust in the device or the technology used, in how the data is dealt with and the trust in the whole system, e.g. the whole HuMan system including the technologies, services, organisations and people [21]. Most frameworks that address trust and privacy look at online systems and trust in the system. In the context of HuMan, there is a strong emphasis of trust beyond the system, but in the organisation and among individuals. Privacy networks identify the receiver of the information and the type of information shared as important precisely because a person may share some information with people they trust, but not with ones they don't trust and this central idea has influenced the design of our framework. In addition, the literature and guidelines available on complying with the GDPR regulations draw attention to transitions in the use of data such as when storing data or transferring the data from one place to another.

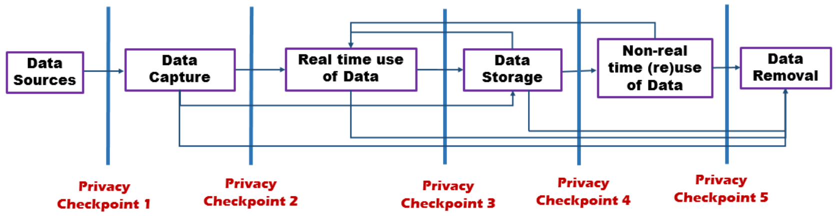

Figure 1 HuMan Trust and Privacy Framework

Drawing from these, we can see the relevance of analysing the data element and its lifecycle as it flows through the system, to determining how to design for privacy. The privacy requirements depend on what you do with the data and who does what. Hence, depending on what the HuMan system or the service does with which data, the privacy design has implications. Thus, we have analysed a data element, from the source and the capture of the data to the end of its lifecycle, illustrated in **Error! Reference source not found.**. We have examined closely what happens when data transitions from one phase to another, and the implications for ensuring privacy across each of the transitions. We have called these Privacy Checkpoints. An early version of the framework was presented in [22].

3.1 Privacy Checkpoints

The Privacy checkpoints provide guidelines for designers and developers to take the necessary precautions and actions for ensuring IT systems and services that protect privacy of individuals and organisations, and foster trust among the workers and in the organisation. The Privacy Checkpoints and how they can support the design of privacy through the data transitions are explained in the following paragraphs. Detailed guidelines have been developed for each checkpoint and we refer to examples of these in Section 3.2.

Privacy Checkpoint 1 – enhances awareness of specific things that need to be ensured every time a data element is captured by any means. The data originates at a source, which may be a workplace, a human worker, or other; e.g. environment. Data may be captured from any source, by a variety of ways. Data may be captured without the source being aware of it or with the consent of the source, automatically by technology (e.g. sensors or cameras) or manually.

Privacy Checkpoint 2 – helps to identify the guidelines that are relevant for the real-time or near real-time use of data (e.g. to provide support to a worker or to provide personalised and timely feedback), store data without being used real-time or removed from the system.

Privacy Checkpoint 3 - identifies the guidelines that are relevant when storing data and for ensuring the security of the stored data. If the data is stored , it may be used for a different purpose. Data storage requires attention in many ways such as informing the data subject and obtaining consent, how long it will be stored for and who may have access to it. Most importantly, the anonymisation and indeed ensuring that the data source or data subject cannot be identified through the data. Particularly, the abundance of third party data storage services, such as the cloud-based storage services, has called for increased awareness of privacy and data security issues.

Privacy Checkpoint 4 - provides guidelines when stored data is used. Stored data may be used as single data elements or/and aggregated with other data elements, perhaps from different sources, to make sense of various contexts and situations. Use of stored data calls for a careful evaluation of what data is used, how, for what purpose and by whom, to ensure privacy and to foster trust in the organisation(s) that collect, use and store the data.

Privacy Checkpoint 5 - provides guidelines on how data should be removed from a system. Data may be removed due to various reasons; e.g. by someone, it may have expired or be ported to another storage system. An important criterion when data is captured or stored is to obtain consent, which encompasses many dimensions such as for how long a data element can be kept in storage. As such, a data element may have a date that determines when the data is not valid any more (or expires) or should be deleted from the system. Deletion or removal of a data element has requirements beyond just deleting data element as to respect privacy; it means all traces of that data element and its links to other entities must also be removed.

As seen from **Error! Reference source not found.**, every single data element does not always follow the complete sequence or all the transitions that have been identified for the lifecycle. For example, the data may be stored with being used real-time or the data may be removed at any point in the lifecycle of a data element; it may be deleted right after it's captured, after real-time use, after storing and without reuse or at any time while it's in storage. Thus, the Privacy Checkpoints provide awareness and guidelines for developers that should be followed prior to any activity on the data; e.g. Privacy Checkpoint 1 applies before any data is captured and similarly, Privacy Checkpoint 5 applies before any data is removed. So, independent of when the data is removed (e.g. after capture or from storage), the guidelines should be considered.

3.2 Applying the Framework to HuMan Services

The HuMan cognitive system and the services address personal data through all the transitions that are captured in the HuMan TPF, illustrated in Figure 2. We will focus on two of the services to illustrate the diversity of the type of data the HuMan services require and how the HuMan TPF could be used to support privacy by design.

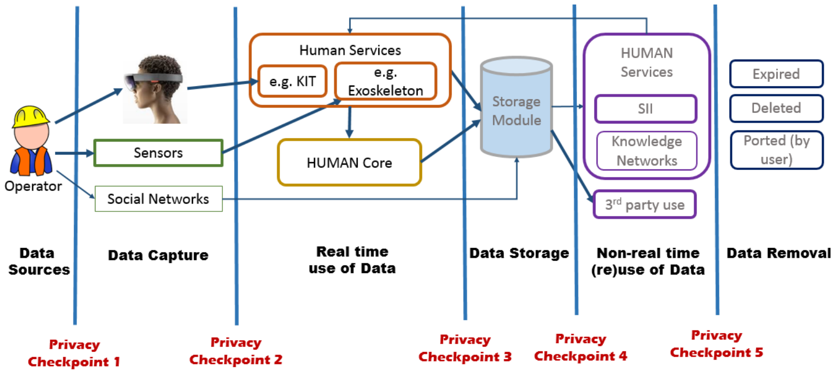

Figure 2 HuMan TPF and services

The Exoskeleton service captures and uses collated data related to a worker's performance of a physical task and physiological conditions and provide real-time support. Physiological data about a worker performing a physical task are captured and monitored to determine if the worker is tired or experiencing physical exertion. Based on the condition of the worker, the exoskeleton intervenes to provide appropriate and timely support for the worker. In this service, real-time data is captured and used real-time. Thus, the guidelines presented in the Privacy Checkpoints 1 and 2 should be considered; e.g. inform the user of data capture, obtain consent, etc. If data is deleted after the work shift, guidelines presented in the Privacy Checkpoint 5 are relevant; but Checkpoints 3 and 4 are not relevant. If the data is stored for secondary use, the guidelines presented in the Privacy Checkpoints 3 and 4 are relevant; e.g. inform the user, obtain consent, ensure data security, etc.

The data that is captured may be stored and used in various ways for supporting workers or improving organisational processes at a later time. This may be done by using single data elements, aggregating data elements and sources, doing correlations or conducting other processes. The SII is a service that processes secondary data to gain insights into the workplace, by applying process mining methods. This framework was first presented in the context of process mining and the SII service in [22]. The guidelines presented in Privacy Checkpoint 4 are extremely important for the SII service; e.g. ensure that consent is obtained for secondary use of data, inform how data will be used, appropriate data security measures, ensure that an individual cannot be identified, etc. For example, a worker's performance against the shift information for the shop floor could help identify an individual. Thus, designing the right privacy in the light of how the data is used is of utmost importance. The HuMan TPF provides support to isolate the specific transitions that the data elements undergo and thus, helps to draw attention to the important and specific design issues at hand for any situation.

4 Threats, Opportunities and Needs: Users' Perspectives

The users were represented by either middle managers that understood the workers' and the organisation's perspectives and/or researchers working with them. The data presented in this section was collected from two separate events; the threats and opportunities workshop and the workshop where the HuMan TPF was used. In the threats and opportunities workshop, the data was gathered using post-it notes, on two large sheets of paper; one for threats and one for opportunities. For the workshop where the HuMan TPF was used, a list of risks was gathered on a large sheet of paper.

The threats and opportunities identified by the use case partners and others were diverse and spanned over several dimensions: e.g. individual/personal and organisational; internal (within the organisation), which could be among peers or between employer and employee, and external (or third parties, such as insurance companies or trade unions); technical and non-technical such as organisational processes or cultural and short and long term perspectives. An important observation was the perception of people and how the workers perceived their privacy and threats to them. This is no surprise as supported by the studies by Adam and Sasse (e.g. [17]). It has to do with their perceived value of the data and how it is used by the organisation. Interesting discussions took place on how things that are initially perceived as threats could be turned around to opportunities, by both technical and non-technical solutions. The discussions resulted in the identification of several opportunities and benefits that could be leveraged from data collection, as shown in Table 1.

In addition to the explicit threats and opportunities, some of the contents from the workshops can be interpreted as needs which can be translated as technical and organisational requirements. These needs are summarised below:

- The workers would like to have control of their data; e.g. decide if they want the data to be collected and who has access to their data.
- The workers perception of the value of the data as well as risks associated with data collection need to be managed.
- The workers' concerns on how the data will be used by others and the organisation need to be managed. A major part of this is fostering and managing the trust between the worker and the organisation.

- The workers' feelings, attitudes and perceptions, which is related to cultural and social aspects. This also requires attention to trust building and managing trust.

Table 1 Users' perspectives: threats and opportunities of data collection

	Threats	**Opportunities**
Individual	• Misuse of data and informatic • Health and safety • Security • Vulnerability • Intrusion (by technology)	• Enhanced knowledge • Knowledge sharing • Accelerated learning and performance improvements • Personalised support and services • Recognition from others and the organisation • Benefits of new analyses of data
Organisation (within)	• Misuse of data and informatic • Data Security	• Process improvements • Benefits of new analyses of data • Proactive action • Improved company image
Organisation (external)	• Misuse of data by 3rd parties • Data Security	• Increased awareness in the unions on benefit of data collection

The list of needs identified from the workshop where the HuMan TPF was used are listed below. In contrast to the above needs, references to the specific uses of the data and the transitions, e.g. capture, storage or deletion, possibly indicate the participants' awareness of privacy issues with regard to how the data may be treated and used.

- Choice of which information is recorded (captured) about them, before use and while the service is used.
- Preset privacy profiles for the different stages in the lifecycle, such as for storage, to ease them to select one from an existing set.
- Possibility to erase data.
- Clear distinction between personal/individual data and company data.
- It should not be possible to identify an individual by linking data.
- Data should only be used for the benefit of the user; not for managerial purposes.

5 Privacy by Design: Developers' Perspectives

The data from the developers were collected from the workshop where the HuMan TPF was used. The developers were split into three groups, ranging from 4-6 participants in each group. The groups were formed around the different HuMan services, e.g. the KIT, EXOS or SII. Their tasks were to identify the personal information the services require from workers or the workplace and to discuss solutions by actively practising privacy by design. They were asked to do this by using the HuMan TPF. They were provided a large printout of the framework, illustrated in **Error! Reference source not found.**.

There were a lot of concerns and discussions within the groups. There was a natural cause for concern as many of the HuMan services focus on personalised, timely support, which require personal information (e.g. physiological data) as well as the identification of the individual that receives the support. Solutions that comply with GDPR and meet the privacy and trust needs of the workers require careful attention and detailed insights into how the data will be treated.

Two of the groups used the printouts of the framework that were provided to make notes. The data capture phase focused on identifying the personal data as well as other data that were captured or used from sources other than the workers; e.g. task related data. For the EXOS service, personal data is captured from the exoskeleton as well as from a smart watch. For the real-time use of this data, there were discussions around which data elements were real-time and which were reused from storage and from the results of processing and analyses of other services such as the SII. These discussions raised awareness about the design of the consent from the user, how to make the data usage transparent to the user and how to provide the appropriate choices to the user. It also increased awareness of the design of the service in the case of limited consent from users; i.e. if and when some of the data were not available. This was a reason to address data minimisation and designing the services to be as effective as possible while respecting the GDPR requirement of data minimisation. Drawing attention to the real-time and secondary use of data encouraged developers to think of the data that is required real-time, perhaps for short-term reasoning. It stimulated discussions around which data is necessary to be stored for supporting long-term reasoning or other types of analyses. This may often require making trade-offs with data capturing and the benefits from the services. Awareness of such issues stimulated discussions around the design of consent, privacy settings and profiles.

One of the groups had noted "login" for all the Privacy Checkpoints, indicating that the user should be informed about the use of the data across all transitions and therefore the need for obtaining the appropriate consent from the user. When talking to the developers, it became evident that the login functionality by the user may not be trivial. There may be different use cases or scenarios where a user logs into the system; e.g. to perform work, using the EXOS service, or to look at the data that is stored to see how s/he performed after the work shift. Thus, from a usability perspective, the design of the consent, privacy profile and login functionality did not necessarily appear as discrete functionalities. Another point of discussion was the GDPR requirement on the right to be forgotten when a user requests his/her data to be removed from the system. Furthermore, there were a no. of other design related discussions, triggered both by the nature of the personal information and the personalised services as well as the data transitions and the potential multiple use of data, both real-time and secondary. A detailed discussion of these is beyond the scope of this paper.

6 Feedback on the Framework

After the HuMan Trust and Privacy workshop using the framework, which lasted 1.5 hours, participants were asked to complete a short questionnaire, to obtain feedback about the HuMan TPF and the workshop itself. There were 18 respondents. The questionnaire included statements and the users were asked to indicate how much they agreed with the statements, using a likert scale (Strongly agree, Agree, Neither agree or disagree, Disagree and Strongly disagree). The responses to the 5 statements about the HuMan TPF are shown in Figure 3.

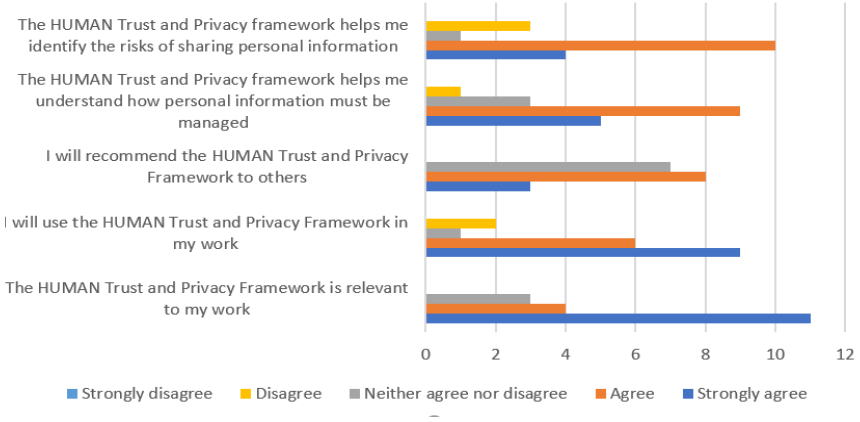

Figure 3 Feedback on the framework

The feedback to the statements that the HuMan TPF is helpful are generally positive; i.e. most participants either agreed or strongly agreed to the statements. However, the responses to the two statements about using and the relevance of the HuMan TPF, indicate that more than half the participants strongly disagreed. For the statement " I will recommend the HuMan TPF to others", 7 out of 18 responded "neither agree nor disagree", but no one disagreed. A possible explanation for the negative results may be the short duration of the workshop and the lack of experience of the participants in using the HuMan TPF.

7 Summary and Future Work

The advent of industry 4.0, with its emphasis on smart factories, relies on the digitisation of the organisation where everything can be measured and tracked, including the human operator on the shopfloor. The advances of technology have opened up new opportunities in decision making and support based on the data that has become accessible. A along with such opportunities, one is faced with the many challenges associated rooted in the privacy paradox where the operator needs to assess what value is conveyed in exchange of loss of privacy.

It is precisely because of the concerns on how personal data is accessed, processed and utilised that has led to legislation on personal data protection, of which GDPR represents the most recent response from the EU to address the abuse and violations on the use of personal data with particular focus on the consumer. However, the difficulty of balancing the concerns associated to the privacy paradox is evidenced in the large number of service providers that are unable to comply with the new regulation and consequently have terminated their service entirely or block service access to Europeans.

The HuMan cognitive system relies on the capture and processing of personal data in order to provide best level of assistance of its services for the operator to carry out their work. To support handling the privacy paradox and encourage the trust of operators in the HuMan solution, a trust and privacy framework was developed. The purpose of the framework is to provide a structured approach to develop the HuMan solution by ensuring that one is aware of the different privacy checkpoints along the lifecycle of personal data, from the point of capture to the removal from the system. By providing a framework, a dialogue with different stakeholders within an organisation can be supported and the developers, all of whom may not be aware of the implications of collecting, processing and storing personal data. Not all the associated guidelines and recommendations have a direct impact on software being developed, with many addressing new processes that are required to be put in place by the organisation. In addition to the guidelines, the framework provides support to the analysis of risks, threats and needs from the users' perspectives.

The paper presented the HuMan TPF, which is being used within the HuMan project to support the developers to identify areas where design trade-offs may help to achieve privacy by design. Some of these trade-offs can be summarised as the value and benefit of the service vs. the data that is captured, the quality of the service vs. data minimisation, the level of control given to the user vs. transparency and flexibility and step-wise consent design vs. usability. The framework is used to facilitate a structured dialogue between the users and developers towards building a solution that delivers value with the users being in control of their personal data.

A workshop was organised to evaluate the HuMan TPF by both the end-user organisations and the development team. The discussions during the workshop and the results demonstrate that privacy by design still remains an afterthought by the development team, with very few being even aware of the concerns on privacy beyond having appropriate terms of service with consent, which in many cases would be implied and not explicit. This lack of understanding is no longer compatible with regulation initiatives such as GDPR, which is addressed by the HuMan TPF.

The feedback from using the framework in a workshop is described. Additional workshops are planned to include the operators and workers from the use case partner companies. The feedback will be used to see how the framework could be improved to support both users and developers. Future work will include using the framework actively to raise awareness and to design and develop both technology and organisational services to achieve privacy by design and comply with GDPR regulations.

Acknowledgements. This research is funded by the EU's H2020 research and innovation programme, grant agreement no. 723737 (HUMAN). We thank all participants of the trust and privacy workshops conducted within the context of the HuMan project.

References

1. Warren, S.D. and L.D. Brandeis, *The Right to Privacy.* Harvard Law Review, 1890. **4**(5): p. 193-220.
2. Adams, A. and M.A. sasse, *Users are not the Enemy.* Communications of the ACM, 1999.

42(12): p. 40-46.

3. Carayon, P., *Human factors of complex sociotechnical systems.* Applied Ergonomics, 2006. **37**(4): p. 525-535.
4. Thoben, K.-D., S.A. Weisner, and T. Wuest, *"Industrie 4.0" and Smart Manufacturing – A Review of Research Issues and Application Examples.* Int. J. of Automation Technology 2017. **11**(1).
5. EFFRA European Factories of the Future Research Association, *Factories 4.0 and Beyond: Recommendations for the work programme 18-19-20 of the FoF PPP under Horizon 2020*. 2016.
6. Looze, M.P., et al., *Exoskeletons for industrial application and their potential effects on physical work load.* Ergonomics, 2015. **59**(5): p. 671-681
7. Blattgerste, J., et al. *Comparing Conventional and Augmented Reality Instructions for Manual Assembly Tasks*. in *PETRA '17*. 2017. Rhodes, Greece.
8. Kokolakis, S., *Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon.* Computers & Security, 2017. **64**: p. 122-134.
9. Stevenson, D. and J. Pasek, *Privacy Concern, Trust, and Desire for Content Personalization* in *The 43rd Research Conference on Communication, Information and Internet Policy Paper*. 2015.
10. *HUMAN Project*. 2017 [cited 2018 1 May 2018]; Available from: https://www.sintef.no/en/projects/human/.
11. EU GDPR Portal. *GDPR Key Changes: An overview of the main changes under GPDR and how they differ from the previous directive*. [cited 2017 23 November]; Available from: https://www.eugdpr.org/key-changes.html.
12. The Nordic Cognizant Blog - The Business Journal of Cognizant Nordic, *GDPR is more than just rules - it's about trust.*
13. van der Aalst, W.M.P., *Process Mining - Data Science in Action*. Second Edition ed. 2016: Springer.
14. Nissenbaum, H., *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. 2010, Stanford, California: Stanford University Press.
15. Ziegeldorf, J.H., O.G. Morchon, and K. Wehrle, *Privacy in the Internet of Things: threats and challenges.* Security and Communication Networks, 2014. **7**(12): p. 2728-2742.
16. Solove, D.J., *A Taxonomy of Privacy,* University of Pennsylvania Law Review, 2006. **154**(3): p. 477-560.
17. Adams, A. and M.A. Sasse, *Privacy in Multimedia Communications: Protecting Users, Not Just Data*, in *People and Computers XV—Interaction without Frontiers (Joint Proceedings of HCI 2001 and IHM 2001)*, A. Blandford, J. Vanderdonckt, and P. Gray, Editors. 2001, Springer-Verlag: London. p. 49-64.
18. Barker, K., et al., *A Data Privacy Taxonomy*, in *British National Conference on Databases, BNCOD 2009*. 2009, Springer International Publishing.
19. Riegelsberger, J., M.A. Sasse, and J.D. McCarthy, *The Mechanics of Trust: A Framework for Research and Design* Intern. J of Human-Computer Studies, 2005. **62**(3): p. 381-422.
20. Dibben, M.R., S.E. Morris, and M.E.J. Lean, *Situational trust and co-operative partnerships between physicians and their patients: a theoretical explanation transferable from business practice. QJM: An Intern. Journal of Medicine*, 2000. **93**(1): p. 55–61.
21. Daubert, J., A. Wiesmaier, and P. Kikiras, *A View on Privacy & Trust in IoT*, in *Workshop on Security and Privacy for Internet of Things and Cyber-Physical Systems, IEEE ICC 2015*. 2015, IEEE.
22. Mannhardt, F., S.A. Petersen, and M. Oliveira. *Privacy Challenges for Process Mining in Human-centered Industrial Environments*. in *Intelligent Environments*. 2018. Rome, Italy: Springer.