Co-designing Employees' Data Privacy: a Technology Consultancy Company Use Case

Waliyah Sahqani
University of Trento, Aalto University
Espoo, Finland
waliyah.sahqani@alumni.unitn.it

Luca Turchet
University of Trento
Trento, Italy
luca.turchet@unitn.it

Abstract—Employee data is increasingly becoming crucial for organisations to improve workflow and foresight. Furthermore, with the onset of the GDPR law, the MyData movement is pushing for human-centric personal data. This presents an opportunity not only to improve how employees can understand their data, but also have transparency and control over it. This paper investigates how a collaborative design process was used at a technology consultancy company to design a service aimed at enabling data transparency and control as well as at communicating its value. We collected qualitative data from a survey, interviews, and workshops conducted with employees. We then built a prototype and tested its usability using a questionnaire. Results showed a clear need among participants for transparency. Results also showed the effectiveness of the prototype in positively enhancing transparency and in generating a good level of usability. The adopted process also led to the formulation of data categories to improve the service's comprehensiveness. Taken together, our results highlight how the proposed model of co-creative design may aid complex transformations in large technology organisations. We provide a set of recommendations in this space and envision future directions for our study.

I. INTRODUCTION

The issue of personal data privacy is timely and important. The onset of the European Union's General Data Protection Regulation (GDPR) forced many organisations to become more transparent and rethink how personal data was being used in their companies. Individuals also became more aware about the use of their individual data as a consumer [1] yet being sceptical about whether companies would implement GDPR practices. Initiatives like MyData Global are driving implementation of personal data rights through its work to "empower individuals by improving their right to self-determination regarding their personal data" [2]. It is an organisation helping personal data become more user-centric through conferences, publications, community building and helping organisations transition to adopt MyData principles from within.

The GDPR law is quite extensive in providing individuals with control of their data and has inevitably transformed data into a valuable entity now, giving rise to the data economy. As "data continues to grow, the data economy will continue to emerge and enable companies to sell and exchange data" [3]. It has opened up a new world of possibilities where data can be used to enhance experiences, build new business models or develop new machine learning and AI technology. However, it

is also a slippery slope that puts privacy at risk and development of a fair data economy is crucial so as to not bring discrimination or privacy invasion into this new setup [4].

As a result, personal data management tools have become popular to exchange, manage and use personal data in various ways (see e.g., digi.me, Meeco, 360ofme, HubofAllThings and BitClave). Companies are helping consumers through such MyData services that provide transparency, control and value. However, one use case is largely ignored which is the subject of this study: organisations' and employee's data. One may wonder, what is the need for utilising employee data in any form? For many companies investing in new technologies like machine learning and AI, personal data coming from various sources (messaging applications, locations, emails, calendars, hour marking as employees) can provide detailed insights into workflows and other aspects of work life that can be recognised and improved. Organisations are recognising that data can help them find new ways to improve efficiency and create better teams.

As exciting as the use cases of building data-driven teams and futures is, it brings huge risks to privacy. One reason being that there is much that is unknown about how processing of data affects privacy. Data about one individual employee may be simple to understand. However, what happens when that individual's data is put in relation with another employee's data to tell a whole new story? This combining of data eventually leads to "things being inferred about us" which "can have a range of effects on our personal agency and more broadly on society as a whole" [5]. Employee's data analysis could sometimes cause some managers to assume one situation over another without understanding the real cause behind the data [6], which can be devastating for employees. Principles and guidelines like those reported in [7] can help navigate this space as a starting point but do not offer specific, tangible solutions to address the balance between data privacy and value driven by data in the workplace. Accenture's report on organisational trust reported that only 29% of businesses co-create policies on organisational and employee data with individuals and this highly indicates a need for this design process [8].

This paper documents the process of co-designing the user experience and interaction of an employee's MyData service in the context of employee and organisational data. Such a process was conducted at a Finnish technology consultancy

company that has operations across Europe. We first survey related works on which our research questions are grounded. Secondly, we detail our methodology, based on collaborative design, which led us to create a concept prototype. The proposed study aimed at designing a service focused on employee data considering the perspectives of privacy, design and collaboration.

II. RELATED WORK

A. Legal aspects

The GDPR law (Recital 155) allows employee data collection under certain conditions, but these conditions are not uniformly defined [9]. We can still not find in GDPR the exact cases or design guidelines for which the collection and processing of data could be allowed as data collection becomes more invisible [10]. We will explore here how to expand these when companies are trying to become data-driven.

Ensuring "private zones" for employees is necessary even during work, but it has become more difficult as processes become digital and technology more invisible [11], [12]. Therefore, organisations need to create policies and guidelines together with their stakeholders which we will explore. It is also important that "an employer must have a transparent system of monitoring, of which all of the employees are fully aware" [12].

B. Employee Data Usage and Organisational Trust

The use of employee data is the crucial part of the service to be designed, so it is imperative to understand how employees feel about the use of their data in organisations. The study reported in [13] investigated employees' perceptions of the use of employees' data by the employer by considering five different multinational companies and their employees. The study showed that employees lacked factual knowledge about what personal data the organisation had about them: there was a huge lack of transparency about this data, different types of data were deemed to be of different sensitivity levels and there was also a sizable group of "I don't know" responses. In general, it was crucial for employees that permission should be asked for whichever use of personal employee data.

Since the context we are researching in is within organisations, the aspect of trust must be looked into deeply. Trust is the basis for individuals feeling comfortable with their data use. The Edelman Trust Barometer mentions a strong positive relationship between the transparency in organisations to the trust in them by their employees echoed by studies in [14], [15]. The survey reported in [14] revealed that trust and transparency are strongly correlated for employees.

C. Designing transparency

Building trust requires transparency, and in the context of human-computer interaction (HCI), transparency-enhancing tools (TET) provide a great starting point to enable informed consent and inform about data usage. Ex post transparency is especially relevant here as it refers to how the data subject has

a right to know how their data is being used and processed [16]. TET research for Data Track and A4 Cloud provide guidelines for how users prefer to have their data usage information available with strong preferences to visual indicators having better usability. In another experiment, robots are used to measure how transparency can enhance a user's understanding of a privacy policy with regard to data collection which increases with transparency [17]. Just providing simple control for consent to users is not enough (that may cover GDPR compliance), but to enable users to be better informed, transparency of the potential that data usage can bring to them is very important. Human-data interaction also provides a model to use for personal data management, by assessing how the applications communicate legibility, agency and negotiability over data [18]. These have proven somewhat useful in [19] and can be triangulated in our study.

Another aspect is to ensure you can enable the informing of users by collecting and creating user requirements before designing the user interface (UI) itself [20], [21], which will also be employed in our process due to the successes found. At the same time, it is also necessary to ensure users are not overloaded with too much information about privacy of data settings in a way that the decision-making and informed consent can be balanced (as learnt from [22]) so as to avoid the complacency that comes with default privacy choices that are propagating the use of "dark patterns" [23].

D. Usability of Privacy

Privacy policies are the current method through which organisations explain to individuals how and what happens to their data. But they are one of the most non-user-friendly ways to communicate complex information. The study reported in [24] provides an approach to the data economy being applied because of the sheer amount of time it takes to read a privacy policy. Potential ways to reduce the complexity and improve usability for data usage information suggested are abstraction and layering of policies, introducing visual policy icons [25], browser extensions with visuals for consent decisions [26], as well as privacy negotiation and personalisation [27]. These approaches can help inform the design of consent aspects in the service.

E. Privacy by Design

Privacy by Design enables data protection in the design of technology itself based on Cavoukian's principles [28]. The need for a privacy by design approach in a collaborative manner is clear - developers and engineers alone cannot have the answers to designing systems that are privacy-aware, but in fact the stakeholders need to be brought in to develop UIs that they will relate to and understand [29]. Privacy is changing the sociotechnical landscape of society and designers can help address these entangled relationships with critical approaches [30]. A way for making the design contextual is to define guidelines for software developers to conduct privacy interface analyses [31]. Transparent permission systems with the concept of "purpose in permission" [32] is essential to develop such privacy by design systems, given the fact that justifying the use of data for any application seems to be a crucial aspect as defined in the GDPR law as well. The

collaborative aspect of designing is highlighted specifically for such issues in [33], [34], [35], [36]. In designing for a complex issue like employee data in the field of rapidly developing data analytics technology, it is crucial to involve stakeholders because employees' "trust in the future will be dependent on them perceiving data use to be a reasonable expectation" [15].

III. RESEARCH QUESTIONS

From looking at state-of-the-art, some basic assumptions can be made before diving into the design process. We can assume that for organisations and employees to be data-advised, trust needs to be fostered, transparency needs to increase, as well as employees need to be given control over their data and shown the value data can bring. From these assumptions we derived the following research question:

RQ: How do we design a service to develop trust and use data to improve employee's work life?

This can be broken into focus areas to answer more specific aspects:

RQ 1: How might we use transparency for employee data to create informed, data decision-makers?

RQ 2: How might we provide control over their data to employees?

RQ 3: How might we build an understanding of the value of data usage through the transparency?

IV. METHODOLOGY

A. User Research

The user research focused on using two main methods, a data usage awareness survey and co-creative interviews with employees. The survey aimed to gather the current perceptions and awareness about data usage, what employee's comfort levels were towards the data usage, what influence did they currently feel and what influence would they want to have. They were shown options of all the applications that could be used internally to collect data. These would be the main sources of data that need to be assessed for privacy as they can be potentially used in the creation of new data-driven applications for the future. The goal was to understand if employees were aware of which of these data sources are being used, how they think these data sources should be used or categorised, and how much control of them they have.

At the same time, employees were also invited to join co-creative interviews to go in-depth into topics of data usage and value of data-reliant organisations. Eleven participants were interviewed (7 males, 4 females). The interviews lasted 45 minutes on average. All interviewees covered seniority roles. This choice was to ensure that the participant had more knowledge about the types of data that might exist internally in the organisation. This would provide better critical insight as the interviewees would have spent more time in the organisation to know the various touch points of the data generated and also how it might be relevant for their workflow. The interviews focused on understanding the awareness people had about their own data, what value it could bring them through the personal dashboard insights, how it can bring the organisation value while also considering risks, as well as what sort of controls they would like to have when it comes to managing their personal data. Interviewees were given visual prompts to show how data is providing insights in other famous software like Spotify's Year-in-Review and Revolut's RevReview. This provided them with examples so that they could draft their own personal insights dashboards.

B. Workshops

1) Evaluation Workshops

After learning from the user research, design requirements could be generated to create mock-up UIs where user input and evaluation could be beneficial. Three workshop sessions involved four employees each (8 males, 4 females) who volunteered to take part in the study. Each session lasted 2 hours and the entire workshop was conducted using Miro (a real-time whiteboarding tool) so that participants could collaborate in real time together with a video call. The participants who attended the workshops were more diverse than those involved in the interviews as some were from the Finnish office and some from the German office of the company so there could be a more diverse representation of the employees' views.

As suggested in [34], showing some unfavourable scenarios can provoke very useful insights about what participants might feel about data privacy. Thus, the designed mock-ups were trying to show all types of data - personal and company data and also some provocative uses of it. Our method also finds inspiration in the use of various cultural probes [37] and critical design to help define a process more concretely [38]. One imaginary application in the mock-up was made to show that everyone's calendar data and time data would be used to see how people are spending their time. This is quite a privacy-invasive task but can also bring benefits in time efficiency at work - thus, it would be an interesting premise to test in this setting. The workshop was structured into five main parts which the participants were facilitated through. Each part required participants to document their thoughts and ideas into virtual post-its in the Miro board and then each participant would be asked to discuss their written post-its so there can be a dialogue and exchange of ideas.

2) Team Workshop

Using the findings from the ongoing design process, a canvas was drafted to help data-driven application design and development teams to start and continue thinking around the topic of data sensitivity, privacy, risks, as well as value of data usage. This tool was tested to help the development team understand what potential actions need to be taken from the sensitivity point of view in the upcoming development phases. As there is need to create new terminology around these topics, this tool has the potential to increase awareness and understanding of the terminologies proposed.

The 15 participants of the workshop were members of 6 teams developing applications that use different types of data within the organisation, including some employee data that needs to be mapped for sensitivity. The roles of these

participants included Developers, Data Scientists, Designers, Advisors and Researchers.

Essentially this tool should empower the development teams to innovate in a data sensitive manner but this tool itself can be improved as needs evolve. Fig. 1 shows an overview of the structure of this canvas. This canvas can be a living tool to provide transparency into decision-making for how data is used and considered in a sensitive manner as organisations become data-advised. This directly feeds to the enhancement of transparency envisioned and how applications provide value in the research questions.

C. Prototype UI Model

From the workshops, further additions and refinements could be made to the list of requirements and design guidelines and a final prototype was designed using Figma. The prototype reflected a service that provides transparency to data and control over employees' data and was used to validate whether the model and terms used in it are useful, effective and usable. The prototype consisted of the following main parts:

The Dashboard (Fig. 2): Showing all the data sources that exist internally - ranging from messaging applications, human resources data, cloud storage and calendars, for example. This also shows all the applications using the data sources internally in the organisation.

Data Source View (Fig. 3): Showing details about each data source - what fields are used, what type of data it is and where it is used. This is also where users can control where the data can be used directly from the source.

Data Application (Fig. 4): Showing details about data-driven applications in the organisation, how the data is used, how it provides value, what data is used exactly and providing control over the usage of that data.

Quick Guide: A view showing some basic information about what different elements mean in the service.

Feedback button: To let users leave feedback on the service or point out any problems.

Labels & Tooltips: These were used to show the categories the data belonged to for indication of consent actions.

Toggles: To set the permission to use data for a single field of data. These are present in both the data source and data application levels.

D. Prototype Evaluation

The prototype was assessed by experiments that involved 25 participants divided into two groups of 14 super users (users previously involved in the co-design process) and 11 new users (who had not been part of the previous interviews or workshops). The users were given the opportunity to test with anonymity in a remote, unsupervised setting.
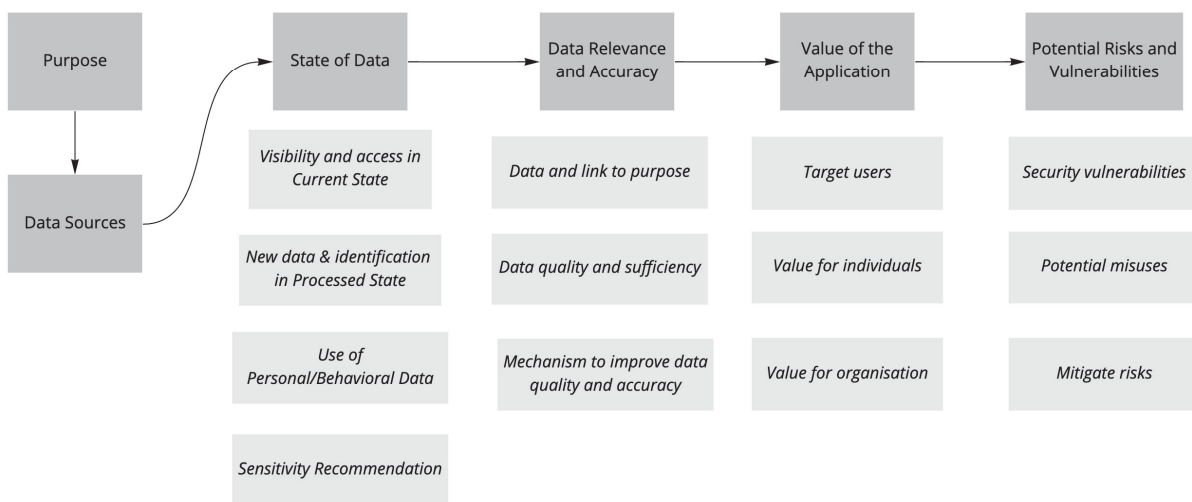

Fig. 1. The Data Sensitivity Mapping Canvas, which guides teams to answer questions about the data used and the value and risks of their data-driven applications
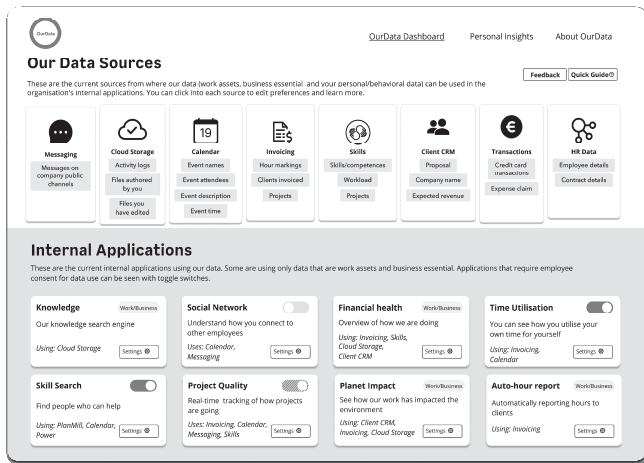
Fig. 2. Dashboard showing all data sources and applications (in Figma prototype)

A remote user testing platform, Maze was used. The user tests were task-oriented with close-ended questions after each task. The tasks for the prototype were structured in the following manner: an introduction to the goals of the prototype, familiarization of the user with the prototype, exploration of the data sources, exploration of how applications use data, changing of preferences for data usage and a free exploration section. To complement these tasks and gather more insight, a set of questions were asked after some of the tasks to gather more quantitative insights about how transparency was enhanced, how much influence users felt they had and how data categorization helped in making informed decisions about consent. Furthermore, we assessed the prototype usability by means of the System Usability Scale (SUS) questionnaire [39].

V. ITERATIVE FINDINGS

A. User Research to Requirements

The results of the survey and co-creative interviews were analysed using affinity diagrams to find recurring themes and give basis to a first set of guidelines and requirements. There were 98 responses to the survey, where the main concentration of responses came from those in pure Developer roles (38 responses) and Designer roles (15) which are the two main competencies present in the company. The interviews were conducted across multiple roles.

Through any transformation that involves technology, employees always need an assurance that the core values remain people first without isolating and pointing fingers. More often people in the survey (and interviews) strongly preferred that data should not be automatically opted in. When asked about how much influence employees felt they had over their data - only 6 employees out of the 98 who answered the survey were fully confident about their influence (see Table I). Very few employees felt they knew where their data was being used, how to find out where their data was being used, as well as how to opt-out if they did not want their data to be used which is a crucial aspect to conceptualise in the design of the service.

In general, most participants were aware that their data was being used internally, with more than 85% of responses stating that their data from the communication application, calendar, skills database and invoicing data is used. This was in line with the current reality in the organisation with regard to internal applications using data from those sources. They also strongly felt that the use of data can only be justified if the value is made clear. Trust was heavily reliant on this aspect of showing employees that there is value in the use of their data.
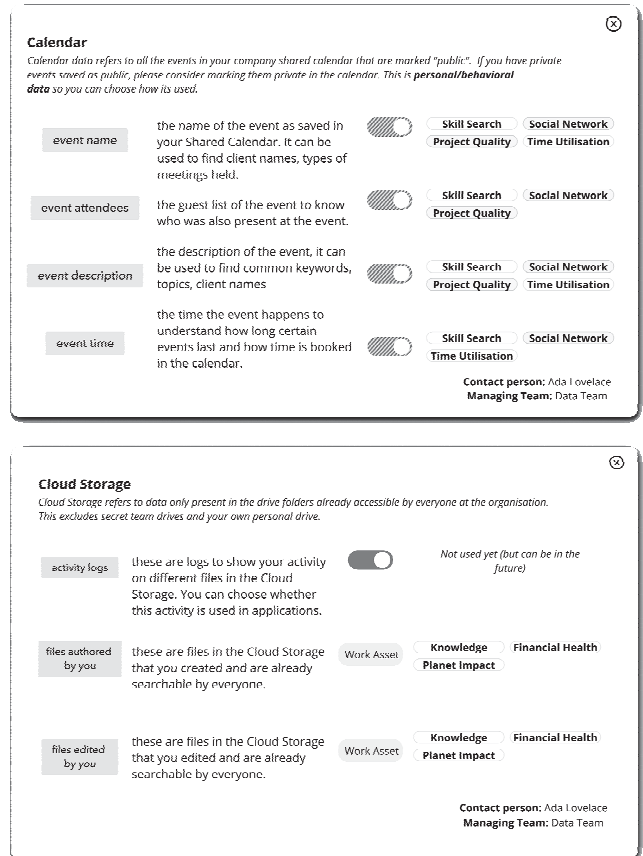

Fig.3. Data sources in detail with fields and consent controls (in Figma prototype)

Respondents felt strongly that data should not be collected if it is not useful, echoing the principles of data minimisation mentioned in Privacy by Design. Many respondents also brought up the concern and scepticism of how the organisation was ensuring data quality and fairness and wanted improved methods to combat this. Employees were also asked to categorise how each of the data sources should be used - they were asked to choose from options: "Do not use", "Use for statistical purposes only (anonymise)", "Use with care - can be sensitive", "Use it, no problem" and "I don't know". There were many varying views on how it should be classified as everyone had different levels of comfort and different opinions, but they believed open dialogue could help improve the way it can be assessed. Most respondents agreed to private data not being used at all, but there was much confusion about many applications that everyone did not use, so it is possible

to infer that knowledge to categorise is also very role-dependant.

The interviews echoed much of the same views but gave a chance to dig deeper into how employees understood value of data. Through the interviews, every single employee was able to ideate personal insights they would like for their work based on data. It was useful for them to understand value of data in their own individual context. In both the interviews and survey, it was clear that building trust requires people to understand how their data is being used. There was a clear request for transparency on data and its usage in the responses in a simple, straightforward way.

B. Workshops

The workshops gave a chance to employees to participate and evaluate mock-ups presented to them showing data sources, various imaginary and real data applications, and consent settings. From these sessions, it became clear that as users, employees thought there was too many decisions for all the data present. Not all data should be opt-out able, but some categorisation should be done to reduce what employees need to consent for as some data is already the organisation's intellectual property or necessary for legal purposes.
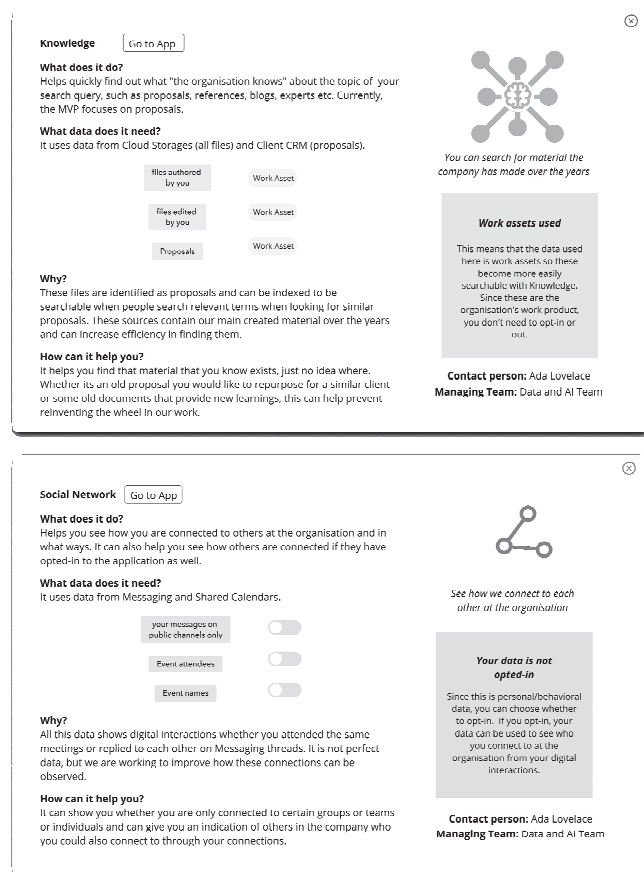

Fig.4. Data applications showing information about the application and consent controls (in Figma prototype)

The mock-ups' style of explaining the value of the data applications was well-received and there was reiteration for design simplicity and consistency to understand new visual patterns. Learning from here, new data categories were created; work assets, business essential (both of which did not require employee consent) and personal/behavioural data (which required employee consent).

TABLE I. THE CURRENT INFLUENCE EMPLOYEES PERCEIVE THEY HAVE OVER THEIR DATA

How much influence do you currently think you have over what data is being used and processed?	Number of Responses
I don't have a very good understanding of what data is used, but I don't need to. I trust organisation handles all of it with care and according to the law.	1
I don't have influence, but I'm informed	21
I feel having influence, but no clear picture of current state.	1
I have influences on some data sources, but not all	27
I have no idea what data is being used, where it is or how to opt-out	39
I have only a little influence. I don't know if I even can opt out of most of stuff.	1
I know but might have trouble remembering. I have seen the opt-out instructions but don't feel the need to opt out	1
I know what data is being used, where it's used and how to opt-out	6
I'm not aware of all the initiatives around these data sources, so I feel I don't have influence. I know I'm able to opt-out from some of them, but don't have any visibility over my data and its use.	1
Total Responses:	98

In the second type of workshop with the team, the main feedback was about how the data sensitivity mapping framework helped teams understand the layers of data involved in their cases. The framework became a living document for decision-making about data which is useful for transparency. Overall, many participants felt they had learnt to add tangible privacy considerations into their work as a result. This qualitative feedback was gathered after the workshop through verbal discussion. The framework was a successful first attempt at making previously, largely legal compliance into a practical and interactive workshop that built more understanding specifically due to the sensitivity recommendations that the canvas provided (see Fig. 5).

C. Prototype Validation

The testing of the prototype was evaluated using the responses to the close-ended questions and overall task completion. Users were asked whether they felt this service enhanced the transparency of data itself. Among new users, 7 out of 11 ranked it at 4 out of 5, and all the super users marked either 4 or 5. Therefore, in general, transparency was enhanced more for super users. For the transparency of data usage, 9 out of 11 new users marked either 4 or 5 but 3 marked it at 3 while among super users, 9 out of 14 marked it at 4 out of 5, while the remaining marked it at 5. This indicates that there is still room for the communication of how data is used in applications to be improved further.

The most important results were that users marked perceived influence over their data more positively than in the original survey (see Table II). In terms of tasks, the average task completion rate was over 70%, which indicates that users were able to get through the tasks independently even in a remote setting with no supervision. When looking at usability aspects, the SUS average score was 75 for new users and 76.8 for super users. These scores are above the passing score of 68 which is very promising given the complexity of the information that was present in the service.

VI. DISCUSSION

One of the main outcomes of the adopted process was the ability to create a model of working with co-design on data privacy, as seen in Figure 6. This led to a constantly updated set of requirements being created containing the goal of the service being envisioned, principles to adhere to, and design guidelines.

The user research and feedback from each stage made it even clearer that transparency enables empowerment among employees. Empowerment means to be able to use the potential of something for one's own advancement and in this case, to be able to use data to do that. The concept of data usage became easier for individuals to grasp through the interviews, workshops and the prototype. They were able to start thinking deeper into what else could be possible and what could be the implications of using data in that manner. This mental unblocking is crucial for the future of data-driven applications. We can conclude there is a positive correlation between transparency of data and its usage to individuals understanding what potential it may have.

Another aspect was the design of the user interface itself and what components in there was important to communicate in terms of transparency, control and value. Through tool-tips with status feedback [40], we made the service more interactive, the toggles helped provide instant control and the informational cards created the transparency and communication needed for people to start understanding how data can be used. To add an improvement to the user experience and usability, it would be worth finding profiles of preference settings that can reduce the time spent in setting up data permissions [41]. This echoes the same concept of data licences provided in [42] and design patterns for sharing data [43].

Overall, the importance of Privacy by Design and organisational trust was highlighted throughout the process. Specifically, in how the data categorisation came about as a need from the employees. It was also put to the test in the data sensitivity mapping workshops with the data-driven team itself as a useful way to abstract the sensitivity of different data.

A. Limitations and future work

There were a few limitations in this work, specifically the number of employees involved was small and stronger results could have been achieved if the pool of employees was larger.

With any study that targets the perception of privacy, it is important to recognise the "privacy paradox" that might exist

as identified in [44]. People tend to be more vocal and concerned about their privacy when prompted, while in reality they do very little to ensure that their privacy is safeguarded.

```
SENSITIVITY RECOMMENDATION #7:
Since there is new data created identifying individuals based on
their personal/behavioural data, consider setting only the use of
the personal/behavorial data as default opted-out for users. This
is personal or behavioral data and they should have the choice to
opt-in if there are new insights being based on identifying
individuals. If there is a way to anonymise the new data,
consider that with a default opted-in setting.
```

Fig.5. Example sensitivity recommendation

For other organisations with similar aims, the existing culture of the organisation is crucial to predicting how employees feel about the use of their data inside the organisation. This research, if done in a company that does not have clearly defined in its culture and practices the need to establish trust and transparency with employees, might yield very different results. In such a case, potentially a lot more employees would be unwilling for their data to be used at all.

The ways this work can be taken forward are multiple, but it would be most important to further explore how personal insights work together with how people understand the value of data through a personal insight's playground. Data quality needs to improve as well, so how can design help create those mechanisms is another possible area to research.

We looked at toggle switches and instant feedback as methods to implement consent, nevertheless, on an infrastructure level, designers need to collaborate with data scientists and engineers to work together to implement data ownership, portability and consent as well. Lastly, further work could be done in how dedicated facilitation for data-driven teams can be useful to avoid privacy invasive technology.

TABLE II. THE EMPLOYEE'S PERCEPTION OF INFLUENCE OVER DATA AFTER TESTING PROTOTYPE

How much influence does this service help you have over what data is being used and processed?	New User	Super User
I have influences on some of my data sources, but not all of my data	6	6
I know what data is being used, where it's used and how to opt-in/out when my data is used	3	8
I don't have influence, but I'm informed	0	0
I have no idea what data is being used, where it is or how to opt-in/out of my data being used	0	0
I'm not sure	2	0
Total	11	14

VII. CONCLUSION

This paper presented a process devised to explore how one could design a user interface for a MyData service similar to the current consumer personal data management solutions but for employees. The service would develop trust and enhance employees' work life through making use of their own and their organisation's data.

Our results highlighted the need for collaborative co-creation with stakeholders on the topic of making data privacy usable in an employee context. We discovered the high awareness of employees in a technology consultancy with regard to the use of their data and learnt that they wanted control over the detailed data fields. The involvement of employees in providing feedback in workshops and user testing helped solidify the value of collaborative design processes as new frameworks of data sensitivity mapping came about as a result of it. Finding the balance between too many and too little choices on data consent was essential to develop this through the constant feedback.

The final validated UI model is a co-creative result of defining user requirements and translating them into a visual form that more feedback can help build further and improve with time. It is just a starting point in how complex issues like privacy can be made tangible through design. A fitting analogy by Harari can help understand the need for work like this - "A self-motivated and well-informed population is usually far more powerful and effective than a policed, ignorant population." [45] And it is the same in the case of employees and organisations. It is more effective and fruitful to have employees that understand how data is used and be informed enough to make the decisions to the best of their knowledge. The development of this knowledge is the responsibility of designers, developers, data scientists and business leaders to come together and be transparent about the work they do and how it can elevate every individual through thoughtful, value-sensitive and innovation-enabling processes.
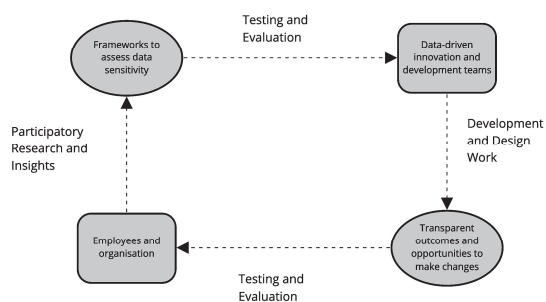

Fig.6. Collaborative and iterative process for data sensitivity for a data-advised future

ACKNOWLEDGMENT

REFERENCES

[1] W. Presthus and H. Sørum, "Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation," *Procedia Computer Science*, vol. 138, 2018, pp. 603–611.

[2] A. Poikola, K. Kuikkaniemi, and H. Honko, "MyData– A Nordic Model for human-centered personal data management and processing," p. 12.

[3] A. Opher, A. Chou, and A. Onda, "The Rise of the Data Economy: Driving Value through Internet of Things Data Monetization," IBM, Web: https://www.ibm.com/downloads/cas/4JROLDQ7.

[4] M. Rantanen and J. Koskinen, "Ethical framework for a fair, human-centric data economy," Sitra, Oct. 2019. Web: https://www.sitra.fi/en/publications/ethical-framework-for-a-fair-human-centric-data-economy/.

[5] "About Data About Us," The Open Data Institute, Sep. 2019. Web: https://theodi.org/article/data-about-us-the-people-know-and-care-more-than-they-are-given-credit-for/.

[6] K. Leong, "Is Your Company Using Employee Is Your Company Using Employee Data Ethically? Data Ethically?" Web: https://hbr.org/2017/03/is-your-company-using-employee-data-ethically.

[7] "10 Principles for Workers' Data Rights and Privacy." UNI Global Union, Web: http://www.thefutureworldofwork.org/docs/10-principles-for-workers-data-rights-and-privacy/.

[8] E. Shook, Mark Knickrehm, and E. Sage-Gavin, "Decoding Organizational DNA," Accenture, 2019, Web: https://www.accenture.com/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-WF-Decoding-Organizational-DNA.pdf.

[9] "Recital 155 - Processing in the employment context," *GDPR.eu*, Nov. 2018, Web: https://gdpr.eu/recital-155-processing-in-the-employment-context/.

[10] C. Ogriseg, "GDPR and Personal Data Protection in the Employment Context," *Labour & Law Issues*, vol. 3, no. 2, 2017, pp. 1-24.

[11] E. Keane, "The GDPR and Employee's Privacy: Much Ado but Nothing New," *King's Law Journal*, vol. 29, no. 3, Sep. 2018, pp. 354–363.

[12] L. Urquhart, "Bridging the gap between law & HCI: designing effective regulation of human autonomy in everyday ubicomp systems," *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct Publication - UbiComp '14 Adjunct*, 2014, pp. 355–360.

[13] J. Adams, D.C. Ganster, M.K. McCuddy, P. D. Tolchinsky and R. W. Woodman and "A Survey of Employee Perceptions of Information Privacy in Organizations," *Academy of Management Journal*, vol. 25, no.3, 1982, pp. 647-663.

[14] B. R. Rawlins, "Measuring the relationship between organizational transparency and employee trust," *Public Relations Journal*, vol. 2, no. 2, 2008, p. 22.

[15] C. Axtell, M. Taylor, and B. Wessels, "Big Data and Employee Wellbeing: Walking the Tightrope between Utopia and Dystopia," *Social Sciences*, vol. 8, no. 12, Nov. 2019.

[16] S. Fischer-Hübner, J. Angulo, F. Karegar, and T. Pulls, "Transparency, Privacy and Trust – Technology for Tracking and Controlling My Data Disclosures: Does This Work?," *IFIP International Conference on Trust Management*, 2016, pp. 3–14.

[17] J. Clark, S. Herse, W. Judge, S. Ojha, M. Tonkin, J. Vitale M. A. Williams, "Be More Transparent and Users Will Like You: A Robot Privacy and User Experience Design Experiment," *Proceedings of the 2018 ACM/IEEE International Conference on Human-Robot Interaction*, Feb. 2018, pp. 379–387.

[18] R. Mortier, H. Haddadi, T. Henderson, D. McAuley, and J. Crowcroft, "Human-Data Interaction: The Human Face of the Data-Driven Society," *SSRN Journal*, 2014.

[19] P. Santos, L. Salgado, and J. Viterbo, "Assessing the Communicability of Human-Data Interaction Mechanisms in Transparency Enhancing Tools," *Federated Conference on Computer Science and Information Systems (FedCSIS)*, Sep. 2018, pp. 897–906.

[20] F. Karegar, N. Gerber, M. Volkamer, and S. Fischer-Hübner, "Helping john to make informed decisions on using social login," *Proceedings of the 33rd Annual ACM Symposium on Applied Computing - SAC '18*, 2018, pp. 1165–1174.

[21] A. P. Felt, "Towards Comprehensible and Effective Permission Systems," 2012.

[22] D. Machuletz and R. Böhme, "Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, April 2020, pp. 481–498, Apr. 2020.

[23] C. Bösch, B. Erb, F. Kargl, H. Kopp, and S. Pfattheicher, "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 4, Oct. 2016, pp. 237–254.

[24] A. M. McDonald and L. F. Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, vol. 4.

[25] S. Fischer-Hübner, J. Angulo, and T. Pulls, "How can Cloud Users be Supported in Deciding on, Tracking and Controlling How their Data are Used?," *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, vol. 421, 2014, pp. 77–92.

[26] Y. Feng, H. Habib, R. Iyengar, V. Bannihatti Kumar, N. Nisal, F. Schaub, P. Story, "Finding a Choice in a Haystack: Automatic Extraction of Opt-Out Statements from Privacy Policy Text," *Proceedings of The Web Conference 2020*, Apr. 2020, pp. 1943–1954.

[27] E. Papadopoulou, A. Stobart, N. K. Taylor, and M. H. Williams, "Enabling Data Subjects to Remain Data Owners," *Agent and Multi-Agent Systems: Technologies and Applications*, vol. 38, G., 2015, pp. 239–248.

[28] A. Cavoukian, "The 7 Foundational Principles," 2009.

[29] O. Ayalon, A. Balissa, M. Birnhack, I. Hadar, T. Hasson, S. Sherman, "Privacy by designers: software developers' privacy mindset," *Empirical Software Engineering*, vol. 23, no. 1, Feb. 2018, pp. 259–289.

[30] R. Y. Wong and D. K. Mulligan, "Bringing Design to the Privacy Table: Broadening 'Design' in 'Privacy by Design' Through the Lens of HCI," *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, 2019, pp. 1–17.

[31] A. S. Patrick and S. Kenny, "From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions," *International Workshop on Privacy Enhancing Technologies*, vol. 2760, 2003, pp. 107–124.

[32] K. Sokolova, "Bridging the gap between Privacy by Design and mobile systems by patterns," 2016.

[33] D. J. Mir, Y. Shvartzshnaider, and M. Latonero, "It Takes a Village: A Community Based Participatory Framework for Privacy Design," *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Apr. 2018, pp. 112–115.

[34] S. Vicini, F. Alberti, N. Notario, A. Crespo, J. R. T. Pastoriza, and A. Sanna, "Co-creating Security-and-Privacy-by-Design Systems," *11th International Conference on Availability, Reliability and Security (ARES)*, Aug. 2016, pp. 768–775.

[35] D. Yoo, A. Huldtgren, J. P. Woelfer, D. G. Hendry, and B. Friedman, "A value sensitive action-reflection model: evolving a co-design space with stakeholder and designer prompts," *Proceedings of the SIGCHI conference on human factors in computing systems*, pp. 419-428.

[36] Y. Yao, J. R. Basdeo, S. Kaushik, and Y. Wang, "Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes," *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, 2019, pp. 1–12.

[37] B. Gaver, T. Dunne, and E. Pacenti, "Design: Cultural probes," *interactions*, vol. 6, no. 1, Jan. 1999, pp. 21–29.

[38] A. Dunne and F. Raby, *Speculative Everything: Design, Fiction, and Social Dreaming*. MIT Press, 2013.

[39] J. Brooke, "SUS: a retrospective," *J. Usability Studies*, vol. 8, no. 2, Feb. 2013, pp. 29–40.

[40] M. S. Aekerman and L. Cranor, "Privacy Critics: UI Components to Safeguard Users' Privacy," *CHI'99 Extended Abstracts on Human Factors in Computing Systems*, pp. 258-259.

[41] J. Lin, B. Liu, N. Sadeh, and J. I. Hong, "Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings," *10th Symposium On Usable Privacy and Security,* 2014, (pp. 199-212).

[42] P. Jurcys, C. Donewald, J. Globocnik, and M. Lampinen, "My Data, My Terms: A Proposal for Personal Data Use Licenses, " *Harvard Journal of Law & Technology Digest*, vol. 33, 2020.

[43] "Data Patterns Catalogue," IF, Web: https://catalogue.projectsbyif.com/.

[44] B. Brown, "Studying the internet experience," *HP laboratories technical report HPL*, vol. 49.

[45] Y. N. Harari, "Yuval Noah Harari: the world after coronavirus," Mar. 2020, Web: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.