Between Privacy Protection and Data Progression: The GDPR in the context of People Analytics

Nella Junge[1]

ABSTRACT

New analytical capabilities have revolutionized the field of Human Resources (HR). With the incessant creation of data and data sources, a new field of practice has developed: people analytics. However, people analytics raises crucial privacy concerns for employees. The new General Data Protection Regulation (GDPR) is supposed to provide more transparency and stronger protection for individuals. By conducting interviews with experts in people analytics and carrying out a survey with people analytics practitioners, this paper examines how the GDPR can be expected to affect organisations using people analytics and their employees. The results of this research indicate that the GDPR will provide stronger privacy and data protection for employees and still allow organisations to conduct people analytics.

1. Introduction

> *"Privacy is not simply an absence of information about us in the minds of others, rather it is the control over information we have about ourselves"* (Fried, 1990, p. 54)

Predictive analytics was widely unknown until The New York Times published a story on how the department store Target predicted a girl's pregnancy (Mai, 2016). By collecting, analysing, and combining data about the girl's purchase history, Target produced a pregnancy prediction score. Predictive analytics has attracted attention and personal data is increasingly being viewed as a commodity and a new resource driving the economy (Mai, 2016). The story of Target demonstrates on the one hand how the increasing availability of data combined with technological advancements has unlocked the potential of data analytics, yet, on the other, reveals the risk of (public) disclosure of private information.

Data analytics has revolutionised the field of Human Resources (HR) by offering an evidence-based approach towards decision-making. With the incessant creation of data, made available by advances in data processing technologies and new emerging data sources such as mobile devices or social media, a new field of practice has emerged: people analytics – also called HR analytics or workforce analytics. As a new data-driven approach to HR Management (HRM), people analytics describes the process of collecting and analysing data from a variety of sources to identify patterns and predict outcomes, which are meant to serve the interests of organisations and employees (Sprague, 2015).

People analytics is assumed to provide an opportunity for HR by supporting decision-making and providing solutions to organisational problems. Moreover, it should benefit employees by increasing their productivity. However, people analytics can raise potential privacy concerns for employees during the process of data collection, data processing, and data distribution. Concerns of people analytics potentially

[1] Nella Junge received a bachelor's degree in European Studies at Maastricht University in 2018. Currently, she works at TI People in Hamburg. Contact: nella@knickmann-junge.com

infringe what Fried (1990) defines as informational privacy, the ability of individuals to control how much information is known.

Because the volume and quality of data are growing, the practice of people analytics is expected to acquire more salience. The technology facilitating people analytics is developing much quicker than data protection legislation, which leaves organisations using people analytics and employees involved in legal uncertainty (Schwartz, Collins, Stockton, Wagner & Walsh, 2017). Consequently, data protection regulations are in demand to be updated to address data confidentiality, regulate the use of employee data and protect the privacy of employees in an increasingly data-driven world.

The General Data Protection Regulation (GDPR) came into force on May 25, 2018, to improve the level of personal data protection and to meet the privacy requirements of the current digital environment. The GDPR harmonizes data privacy laws across the EU and takes data protection concerns to EU level. By imposing stricter obligations and requirements for organisations using personal data, the GDPR is supposed to bring more transparency and stronger protection for individuals. For instance, as one of the key principles, the GDPR requires privacy and data protection by design and default, which is argued to be the most stringent implementation of privacy by design (Hintze & LaFever, 2017).

Due to the fact that the GDPR brings new obligations and requirements for personal data-intensive organisations, the question arises what implications the GDPR will have for people analytics. Does the GDPR improve privacy and data protection for employees and thereby limits the usage of people analytics for organisations? Specifically, this study examines the following research question: How can the GDPR be expected to affect organisations using people analytics and their employees? The research is conducted in light of the EU's overall need to find the right balance between protecting privacy and promoting data analytics to encourage innovation and business progression.

Taking an exploratory approach, the research was conducted before May 25, 2018, to examine the anticipated implications of the GDPR at the end of a two-year implementation phase and shortly before the enforcement of the GDPR. This research is based on a two-step analysis. Firstly, anticipated implications for organisations and their employees were preliminary analysed based on both, interviews conducted with experts in people analytics, and secondary literature. Following the preliminary analysis, two hypotheses were established: The GDPR is expected to improve the control of employees over their personal data and their overall influence in people analytics projects (H1). The GDPR is expected to restrict organisations to conduct people analytics (H2). Secondly, a survey was conducted with people analytics practitioners to verify the hypotheses.

Given that people analytics is a recent field of practice and the academic literature yet limited, analysing people analytics in the context of the GDPR provides a point of reference in the development of people analytics and contributes to the academic debate on data protection and privacy. Moreover, the findings of this research could influence future decisions of investment in people analytics. This study is organized as follows: Chapter two reviews the academic debate on people analytics. Chapter three conceptualises privacy in context of the digital age and people analytics. The fourth chapter discusses the GDPR and focuses on its changes. Chapter five outlines the methodology and data collection and incorporates the preliminary analysis to formulate survey questions and hypotheses. The sixth chapter discusses the second part of the analysis, the results of the survey in light of the hypotheses. The last chapter concludes this study.

2. The Academic Debate on People Analytics

This chapter reviews the academic debate on people analytics. On the one hand, it discusses opportunities and benefits which people analytics offers HRM. On the other hand, it addresses potential privacy concerns for employees.

2.1 HR Debate on People Analytics

The term people analytics covers a variety of approaches to HRM but can overall be characterized as the search for new sources of quantitative employee data and the usage of that data to make more informed workplace decisions in an organisation (Bodie, Cherry, McCormick & Tang, 2017). People analytics is a much-discussed topic among the HR community. Organisations increasingly recognize the importance of having the ability to access and analyse the right data to support employee-related decisions (Barriere, 2016).

Many HR professionals predict a promising future for people analytics by arguing that it provides an efficient and effective approach to HRM. It enables HR departments to receive information about employees, which may have not otherwise been apparent (Bodie et al., 2017; van den Heuvel & Bondarouk, 2016). For instance, people analytics allows organisations to answer questions as to which candidate should be hired, what makes candidates join and perform well, or who is at risk of leaving the organisation (Lal, 2015; Sprague, 2015). Based on these insights, it is claimed that different types of management, business and HR decisions can be informed and improved by being less subjective and intuitive and more objective and evidence-based (Baek, 2016; Barriere, 2016; Batra, 2014; Bose, 2009; Chamorro- Premuzic, Akhtar, Winsborough & Sherman, 2017; Cherry, 2016; Momin & Mishra, 2015; van den Heuvel & Bondarouk, 2016).

By analysing how employees work together, it is argued that people analytics provides an approach to make employees more satisfied, more efficient and more productive. Thereby, it serves as a source of employee productivity and business success (Bodie et al., 2017). Google for instance conducts people analytics based on the argument that "accurate people management decisions are the most important and impactful decisions that a firm can make" (Bodie et al., 2017, p. 972). Its HR department uses data to systematically improve employee performance and leadership within the company.

Overall, the literature on people analytics seems mostly dominated by HR consultancies and software suppliers who aim to exploit commercial opportunities. Scholarly scientific research on people analytics is limited (van der Togt & Rasmussen, 2017). People analytics has just recently revolutionized HR and is not yet the standard for HR departments, which could explain the lack of scholarly attention. The scientific literature that does exist on people analytics introduces the new field of research (Barriere, 2016; Batra, 2014; Kim & Hanson, 2016) and refers to the development of HR digitalization and the innovation of predictive analytics (van den Heuvel & Bondarouk, 2016). In addition, the literature focuses on case studies of certain organisations (Bodie et al., 2017) and provides examples of how people analytics can be applied in HRM (Holthaus, Park, Stock-Homburg, 2015; Lal, 2015; Reindl, 2016).

2.2 Privacy Concerns of People Analytics

Data of employees is the key requirement in people analytics. Organisations cannot conduct people analytics without it. Hence, people analytics can raise important privacy concerns for employees. Since people analytics can be conducted at different levels within an organisation, it can raise privacy concerns at different stages. Before this section addresses privacy concerns related to people analytics, it briefly discusses how people analytics can be conducted at different levels using Fitzenz's (2010) five-step value ladder of HR measurement.

Step one marks the start of HR measurement and refers to the recording of HR related work such as hiring, training, supporting or retaining. By measuring efficiency, processes can be improved and value can be created for the organisation. Step two links the recorded work to the objectives of an organisation, which are set periodically and reviewed on a regular basis. Step three involves the process of benchmarking and step four constitutes the first level of analytics. This step is descriptive analytics and defines and describes relationships among data in an exploratory way to understand past behaviour, outcomes, and trends. Analytics can generally be described as the discovery of meaningful patterns in data (Bodie et al., 2017). The final step of people analytics is predictive analytics, which gives meaning to the patterns observed in the previous step of descriptive analytics and aims to predict future likelihoods based on data-based models (Barriere, 2016; Batra, 2014; Bose, 2009; Fitzenz, 2010; Sprague, 2015).

Since organisations aim to move towards predictive analytics which they consider to be the Holy Grail of people analytics (van den Heuvel & Bondarouk, 2016), this thesis demonstrates how predictive analytics can raise privacy concerns for employees. Privacy scholar Daniel Solove has identified three different contexts of predictive analytics in which employees' privacy could be violated: data collection, data processing, and data distribution (Bodie et al., 2017). These three categories are discussed below.

The first category refers to data collection. People analytics practitioners collect and combine personal data from different sources to identify patterns, trends or relationships among data. Based on these insights, decisions are made, or outcomes predicted (King & Forder, 2016; Mantelero, 2016; Shah, 2017; Sprague, 2015). The sources of data have increased, and modern technologies have enabled a more efficient collection and analysis of data across teams, departments and regions regardless of its complexity. Next to the general data required by HR departments, data can be collected from other data sources such as e-mails, organisations' internal social media platforms or from more innovative data sources such as employee ID badges that record the locations or movements of employees (Cherry, 2016). Moreover, individuals constantly emit data through social media such as LinkedIn which could be also used for people analytics (Baek, 2016). Never before have organisations and HR departments been able to know so much about their employees since it has become easier and less expensive to obtain needed information (Bodie et al., 2017; Klosek, 2000). However, the privacy of employees can be violated since the data sources could potentially disclose an employee's private information (Bodie et al., 2017; Sprague, 2015).

The second category refers to data processing, which involves the use of data after it has been collected. There are two main concerns related to data processing. The first one is aggregation, also called data fusion. When data collected from different sources is combined with other data, anonymous data could suddenly reveal intimate and sensitive facts about individuals (Bodie et al., 2017; King & Forder, 2016; Sprague, 2015; Williams, Brooks & Shmargad, 2018). The value of data does not diminish when it is used but can be processed repeatedly for different uses. Thus, the second concern refers to the risk of secondary uses i.e., data being reused beyond the scope of its stated purpose and without the individual's

awareness or control (Bodie et al., 2017; Cecere, Le Guel, Manant & Soulié, 2017; Guenole & Feinzig, 2016; Sprague, 2015).

The third category refers to information distribution and concerns the risk of data obtained legitimately but improperly provided to a third party (Bodie et. al., 2017). While not related to people analytics, the data scandal of Facebook and Cambridge Analytica serves as a recent example, where according to Facebook, personal data of up to 87 million users has been improperly obtained (Forbes Agency Council, 2018). Overall, despite research by Bodie et al. (2017), privacy concerns of people analytics are not extensively discussed in academic literature and are only addressed to the extent that organisations should consider and respect privacy when conducting people analytics. It can be argued that privacy concerns are being marginalized by potential opportunities and benefits people analytics brings to HR. In this regard, this research broadens and contributes to the academic debate of data protection and privacy in people analytics.

3. Conceptual Framework – Privacy

Despite the fact that the right to privacy has long been recognized, concerns about privacy and the protection of personal data have grown in recent years (Klosek, 2000). The increase in privacy concerns appears to be motivated by the widespread usage of technological advances such as computer-based, digital electronic technologies (Bodie et al., 2017; Klosek, 2000; Nissenbaum, 2010). The advancements in technologies and the associated reductions in costs have led to an exponential growth and availability of data and magnified the power of human beings over information (Bodie et al., 2017; Kshetri, 2014; Nissenbaum, 2010). Technology has revolutionized the ability of individuals and groups (organisations, institutions, societies) to generate, store, access, share, communicate and analyse information in historically unprecedented ways. Data has become a new source of economic and social value (Bodie et al., 2017; Nissenbaum, 2010; Tene & Polonetsky, 2013).

Due to powerful new capabilities, systems and practices developed, which radically affect how much information is gathered, how much is known because of the gathered information and by whom (Nissenbaum, 2010). As more personal data is being collected, frequently without consent, and more personal information is known, privacy diminishes (Bodie et al., 2017; Klosek, 2000; Nissenbaum, 2010). Concerns about the privacy of personal data are nothing new and are present since means for transferring and distributing personal data developed (Klosek, 2000). The availability and usage of data systems and practices in the digital age raise privacy concerns which differ quantitatively and qualitatively from earlier privacy concerns (Tavani, 2008a). The amount of personal data collected, the speed at which data is transferred and the amount of time data can be stored have *quantitatively* intensified privacy concerns. The type of personal information which can now be collected, processed and analysed have *qualitatively* changed privacy concerns related to the collection and usage of personal data (Tavani, 2008a).

Two common approaches to conceptualize informational privacy are the restricted access theory and control theory (Mai, 2016; Nissenbaum, 2010; Tavani, 2008b). The restricted access theory characterizes privacy as a constraint on access. It states that an individual enjoys informational privacy when he or she is able to restrict or limit others from accessing personal data (Mai, 2016; Tavani, 2008b). However, the restricted access theory is being criticised for ignoring or underestimating the role of control

or choice that is also required for an individual to enjoy privacy. As the control theory acknowledges the choice of an individual to grant others access to personal information or restrict or limit their access, it goes a step further than the restricted access theory. It characterizes privacy as a form of control over personal information. (Mai, 2016; Tavani, 2008b).

Westin (1976) and Fried (1990) articulate and support the control theory of privacy. Westin (1976) defines privacy as the "claim of individuals … to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 7). Fried (1990) further defines privacy as "not simply an absence of information about us in the minds of others, rather it is the control over information we have about ourselves" (p. 54). Most conceptions of privacy adopted in scholarship, law and policy emphasise control as a component of privacy or argue that privacy constitutes a particular form of control (Nissenbaum, 2010). Moreover, Banjeree (2018) claims that privacy protection in the digital age does not directly imply that data should not be collected, stored or used, but should guarantee that data can only be used once consent and legitimate purposes are given.

People analytics serves as an example of a data practice developed because of new powerful technological capabilities. It exemplifies how privacy diminishes as more personal data is being gathered and more personal information is known. On the one hand, this research is motived by the question of whether the GDPR improves privacy for employees in the context of people analytics. To conduct this research, this study uses the control theory to inform and approach the concept of privacy. Moreover, it sets the research focus on the influence of employees in people analytics and enables an approach to evaluate whether the privacy of employees is secured under the GDPR. It allows to examine whether employees enjoy privacy in the sense of having control or choice over their personal data when organisations conduct people analytics.

According to Nissenbaum (2010), a right to privacy imposes obligations and restrictions on others. The GDPR aims to bring stronger data and privacy protection for individuals by imposing stricter obligations and requirements for organisations. Hence, this study, on the other hand, investigates how the stricter GDPR obligations and requirements for organisations are expected to affect organisations using people analytics. Will the GDPR improve privacy and data protection for employees but limit organisations to conduct people analytics?

4. Changes introduced by the GDPR

Kshetri (2014) and van den Heuvel and Bondarouk (2016) argue that potential privacy concerns of people analytics result in strong pressure on governments to prevent people analytics from a potential privacy invasion. It is argued that data protection laws need to determine whether and how organisations should be permitted to collect and analyse personal data as well as define the scale to which it is reasonable to make decisions and predictions based on that data (Kim & Hanson, 2016; Klosek, 2000; Mai, 2016). This chapter discusses the data protection legislation in the EU.

In general, as the technical possibilities for processing huge amounts of data from multiple sources continue to grow, data protection has turned into a focal point in policy. This has become also apparent in Europe. The former Data Protection Directive (DPD) of 1995 no longer met the privacy and data protection challenges in Europe (Koops, 2014). Back in 1995, just one percent of the world's population was using the Internet. However, the technology has developed severely and today the Internet is almost omnipresent across the EU (Tankard, 2016). Because the DPD was a directive, the EU Member States had different interpretations of data protection and thus, European data protection legislation was fragmented

(Tankard, 2016). Consequently, a consensus was reached emphasizing the need for an updated set of data protection guidelines and a harmonized framework at EU level (Hallinan, Friedewald & McCarthy, 2012).

To meet current challenges related to personal data protection in an increasingly data-driven world, the GDPR came into force and replaced the DPD on May 25, 2018 (de Hert & Papakonstaninou, 2012; Tikkinen-Piri, Rohunen & Markkula, 2018). As a uniform legislative framework at EU level, the GDPR harmonizes data protection across the EU and sets new requirements for personal data-intensive organisations. All organisations collecting, processing, and utilizing personal data of EU citizens, regardless of their location, are required to comply with the new rules and guidelines (Tankard, 2016). In a two-year transition period until May 25, 2018, organisations were given time to review and revise their organisational and technical privacy protection measures (Tikkinen-Piri et al., 2018). Since this research examines how the GDPR can be expected to affect organisations using people analytics and their employees, this thesis addresses solely GDPR changes that are relevant for organisations using people analytics. Therefore, it discusses the GDPR changes which Tikkinen-Piri et al. (2018) identified as the most relevant for personal data-intensive organisations.

In general, the GDPR defines personal data as "any information relating to an identified or identifiable natural person (data subject)" and describes data processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means" (EU Regulation, 2016, p. 33). The GDPR is binding for EU organisations and all non-EU organisations handling EU citizens' personal data or monitoring the behaviour of data subjects within the EU. Non-EU organisations need to comply with both the GDPR and their national legislation and need to designate a representative in the EU (EU Regulation, 2016; Tikkinen-Piri et al., 2018).

As one of the main principles, data protection by design and by default ensures that privacy is considered in every process and enforced throughout the organisation. Organisations need to demonstrate their compliance with the GDPR requirements for instance by setting up codes of conduct. It is obligatory to obtain the consent of the data subject if an organisation seeks to use personal data. Moreover, the organisation needs to inform data subjects about processing operations, the legal basis, data security measures, their rights and the organisation's interest. Furthermore, the minimisation principle requires organisations to limit the processing of personal data to the minimum extent and organisations should be able to specify the needs and usage of data (EU Regulation, 2016; Tikkinen-Piri et al., 2018).

The GDPR has strengthened 'the right to be forgotten', which requires organisations to delete personal data if the data subject demands it. In accordance with the 'right to data portability', an organisation must provide an electronic copy of personal data of a data subject on request. In addition, it is obligatory to maintain a record of processing activities and in case of potentially risky processing operations, organisations need to conduct a data protection impact assessment. Organisations with substantial data processing activities are required to designate a data protection officer (DPO), who needs to function independently of the organisation. In case of data breaches, organisations are obliged to notify data protection authorities and data subjects within 72 hours and can be charged with a fine of up to €20 million or 4 percent of the organisation's annual global turnover, whichever is greater (EU Regulation, 2016; Goddard, 2017; Tankard, 2016; Tikkinen-Piri et al., 2018). These changes suggest that the GDPR

strengthens privacy and data protection for data subjects, while imposing stricter obligations and requirements for organisations. To examine what implications these GDPR changes will have for people analytics, this study analyses how the GDPR is expected to affect organisations using people analytics and their employees.

Existing literature mainly focuses on general information of the GDPR, changes compared to the former DPD, as well as reasons why a new data protection legislation was needed (Albrecht, 2016; Goddard, 2017; Tankard, 2016; Tikkinen-Piri et al., 2018). It can be expected that now that the GDPR is enforced, its academic discussion increases. Criticisms on the GDPR are only partly discernible (de Hert & Papakonstantinou, 2016; Koops, 2014). Koops (2014) claims that the GDPR entails three fallacies: the delusion that a data protection law can give individuals control over their data, the misconception that the reform simplifies compliance, while in fact, it complicates it even more, and the assumption that data protection law should be comprehensive. Moreover, de Hert and Papakonstantinou (2016) argue that the GDPR takes an outdated approach as it claims that the processing of personal data could be an identifiable, single and standalone operation.

Nevertheless, the extent to which the GDPR successfully fulfils the current challenges related to personal data protection in the EU goes beyond the scope of this study. The existing literature on the GDPR demonstrates that the GDPR has not yet been analysed in the context of people analytics. Hence, this research contributes to the existing academic work by analysing how the GDPR is expected to affect organisations using people analytics and their employees.

5. Methodology and Data Collection

This research is based on qualitative and quantitative sources. It was conducted from March 2018 until May 25, 2018, to examine the anticipated implications of the GDPR for people analytics at the end of the two-year implementation phase and shortly before the enforcement of the GDPR. Since the academic work on people analytics is limited, interviews were conducted with experts in people analytics to broaden the knowledge next to insights gained from secondary literature. As research based solely on secondary literature and interviews could be criticised for lacking validity and objectivity, this research is based on a two-step analysis.

Firstly, based on the interviews and secondary literature, anticipated implications of the GDPR for organisations using people analytics and their employees were analysed and hypotheses were formulated. As the purpose of this preliminary analysis is mainly to formulate hypotheses and to set the framework of a survey, it is incorporated into this chapter. Secondly, the results and hypotheses of the preliminary analysis were consolidated within a survey conducted with people analytics practitioners to assess whether they can be confirmed or rejected. This way, the analysis is based on three data sources: secondary literature, interviews, and a survey conducted with people analytics practitioners. This allows for triangulation improving the objectivity and validity of this research.

Since this research was highly dependent on responses, the case selection had to be left quite broad to maximize the response rate. Nevertheless, the focus is set on large organisations because, so far, rather large organisations have started to conduct people analytics and have more people analytics practitioners employed. Moreover, Kshetri (2014) argues that risks associated with owning and storing data are likely to increase with the size of data and thus provide better privacy related insights.

5.1 Interviews

The author conducted structured interviews with Participant A on April 16, 2018, and Participant B and C on April 24, 2018. The author selected them based on their experience and expertise in the field of people analytics. Participant A is an author, speaker and influencer in HR strategy, people analytics and the future of work. In 2014, he was listed as one of the "15 HR and People Analytics Experts to Follow" (Beyond HR Forum, n.d.). Participant B is a HR leader with more than 15 years of experience in people analytics, talent management, workforce planning and driving innovation across HR. Participant C is a writer, speaker and executive consultant on people analytics, data-driven HR and the future of work. As recognized as one of the most influential people analytics experts by the community, he won many accolades and is regularly being included in influencer lists on people analytics (HR Tech Summit, 2018).

All three interviewees believe in a future of people analytics and can thus be assumed to be in favour of people analytics, which should be considered in the analysis of anticipated implications of the GDPR for people analytics. However, the interview questions were influenced by secondary literature which is informed by the discussion of privacy concerns of people analytics. Thus, the results of the interviews combined with academic literature enabled an objective framework on which the survey could be developed. The sample size was limited to three interviewees since the interviews provided sufficient expertise and insights to supplement the secondary literature. Moreover, the interviews are complementary to the secondary literature and the survey. The interview questions followed from the gap of the secondary literature and mainly focus on the anticipated implications of the GDPR for people analytics. Interview transcripts are available upon request.

5.2 Formulation of Hypotheses

This section presents the preliminary analysis based on the interviews conducted and secondary literature. It firstly discusses the anticipated implications of the GDPR for employees and secondly, examines the anticipated implications of the GDPR for organisations using people analytics. For each part, a hypothesis is formulated.

According to Tikkinen-Piri et al. (2018) the GDPR aims to meet the current challenges related to personal data protection. Following the new GDPR requirements and obligations such as the obligation to obtain consent, the GDPR is specifically expected to provide individuals with better capabilities for controlling and manging their personal data (Tikkinen-Piri et al., 2018). The results of the interviews show that the experts in people analytics expect the GDPR to improve privacy and data protection for employees as well. Participant A argues that "the GDPR is an excellent legislation that brings protection to employees". Most notably, the experts emphasize that the obligation to obtain the consent of data subjects is expected to increase the say and control of employees over their personal data. Participant C claims "it gives the employees more say on the data that is collected, stored and used". Participant A agrees and states "giving employees the chance to opt in as a requirement of the GDPR to have their data stored, used and given to a third party is in my view very welcome".

Since organisations must be able to specify the reasons for the usage of employee data and are obliged to obtain the consent of employees, Participant B and A argue that the privacy concern of employees of secondary uses, i.e., data being reused beyond the scope of its stated purpose and without

their awareness or control is limited. Participant C further claims that the GDPR will force organisations using people analytics to start thinking about the employee rather than just the business outcome. He believes that "if you cannot articulate the benefits to the employee, then maybe you should not do the people analytics project". Likewise, Participant A argues that the GDPR will increase the influence of employees as organisations need to properly and appropriately undertake people analytics projects from a people's perspective. Moreover, the participant claims that the GDPR clarifies the business parameters for people analytics projects up front.

As anticipated in the discussion of the changes introduced by GDPR, the results of the interviews and the arguments in the academic literature suggest that the GDPR is expected to affect employees in a way that it improves the control of employees over their personal data and their overall influence in people analytics projects. Hence, this study establishes the hypothesis that *the GDPR is expected to improve the control of employees over their personal data and their overall influence in people analytics projects (H1).*

This study further investigates how the GDPR is expected to affect organisations using people analytics. Hintze and LaFever (2017) claim that people analytics and other uses of personal data will be impractical, incompatible or at least more difficult under the GDPR. They argue that stricter data protection obligations and requirements, the establishment of new rights for data subjects and the need to adopt new technical measures and practices to ensure the organisation's compliance will challenge the practice of people analytics. They further claim that organisations using people analytics will either have to comply with the GDPR requirements but face significant limits on data usage and data value or will be charged with high fines for non-compliance (Hintze & LaFever, 2017).

Participant C agrees that a potential risk exists that an organisation will not be compliant with the GDPR requirements and charged with financial penalties, which are more stringent than before. Furthermore, the GDPR is expected to challenge organisations using people analytics, for instance, by demanding time to obtain individual consent for each data subject or limiting data usage to the minimum extent (Hintze & LaFever, 2017). The experts in people analytics further argue that there is a potential risk that the GDPR will limit the use of data, its value and the amount of data required for organisations to conduct people analytics. Participant C reasons, "the less data the people analytics team has got, the harder it is to do people analytics".

Participant A points out that people analytics practitioners could feel that the GDPR imposes too heavy restrictions to achieve business objectives. Following the arguments in the academic literature and the results of the expert interviews conducted, it can be expected that the GDPR restricts and carries risks for organisations using people analytics. Hence, based on this preliminary analysis, this thesis establishes the hypothesis that *the GDPR is expected to restrict organisations to conduct people analytics (H2).*

5.3 Survey

The findings and hypotheses of the preliminary analysis are tested by a survey conducted by people analytics practitioners. The author contacted people analytics practitioners from organisations through LinkedIn based on the convenience sample, which means the sample size was based on the willingness of the target group to participate in the study. The survey was conducted until May 25, 2018, to examine how people analytics practitioners anticipate the GDPR to affect organisations using people analytics and their employees at the end of the two-year implementation phase and shortly before the enforcement of the GDPR. The author contacted 300 people analytics practitioners on LinkedIn, of which 41 people responded. Participants who did not finish the survey (N=16) were omitted, which left 25 participants in

the sample. All people analytics practitioners who participated in the survey are employed by different organisations.

The survey questions constituted closed questions to increase the likelihood that the survey would be completed. A major challenge related to the implementation of the GDPR is the lack of awareness and understanding of the new changes and requirements of the GDPR by organisations (Tikkinen-Piri et al., 2018). To increase the validity of the subsequent survey questions, the survey integrated an introductory question referring to the respondents' knowledge of the GDPR requirements and obligations using a 5-point Likert-type scale ranging from 'extremely' to 'not at all'. In case a respondent was not at all informed about the new obligations and requirements of the GDPR, the survey ended.

The people analytics practitioners were asked to select those of the implications discussed in the preliminary analyses, which they expect the GDPR to have on employees and organisations using people analytics. The questions allowed for multiple answers. Since one of the main benefits expected for employees is the improvement of privacy and data protection, the survey additionally measured how people analytics practitioners value data protection compared to business outcome. Moreover, the people analytics practitioners were asked for their general opinion on the GDPR.

As non-compliance constitutes an anticipated risk for organisations using people analytics, the survey investigated which of the GDPR requirements organisations have prepared for and comply with. The question allowed for multiple answers as well. Moreover, the survey measured how overall aligned the organisations are with the GDPR, and how overall worried the people analytics practitioners are about their organisation being non-compliant. The survey ended with demographic questions and is available upon request.

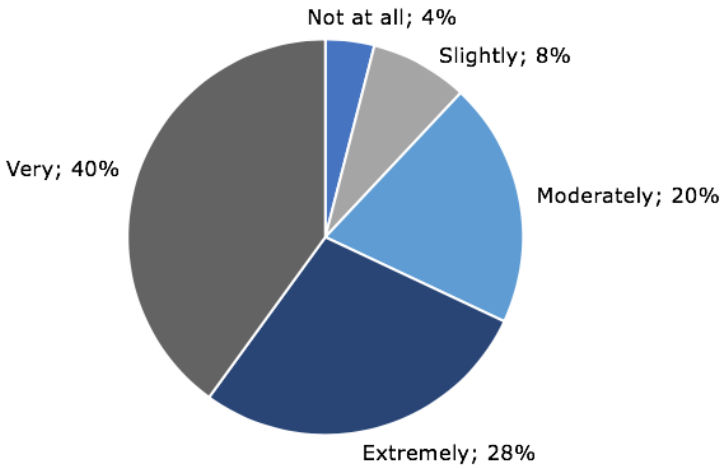
6. Results and Discussion

This chapter analyses the results of the survey and examines whether the findings of the preliminary analysis rather support or reject the two hypotheses. The results have been analysed using Microsoft Excel. Figure 1 shows how informed the people analytics practitioners are about the new GDPR requirements and obligations. It reveals that the majority of the respondents are very informed. 88 percent of all respondents are moderately, very or extremely informed about the new GDPR requirements and obligations, which does not confirm the concern that people analytics practitioners lack awareness and understanding of the new changes and requirements of the GDPR. It can rather be assumed that most of them have sufficient knowledge to answer the subsequent questions, which increases the validity of the survey.

Overall, this study examines how the GDPR can be expected to affect organisations using people analytics and their employees. Figure 2 shows which anticipated implications, discussed in the preliminary analysis, the people analytics practitioners expect the GDPR to have for employees. Overall, it can be observed that there is a strong tendency of people analytics practitioners to agree with the findings of the preliminary analysis. As emphasized in the interviews and in academic literature, the majority of the people analytics practitioners (92 percent) expect the GDPR to improve privacy and data protection for employees and to increase the say and control of employees regarding the collection, storage and usage of their data (90 percent). Most of the people analytics practitioners also expect the GDPR to increase the influence of

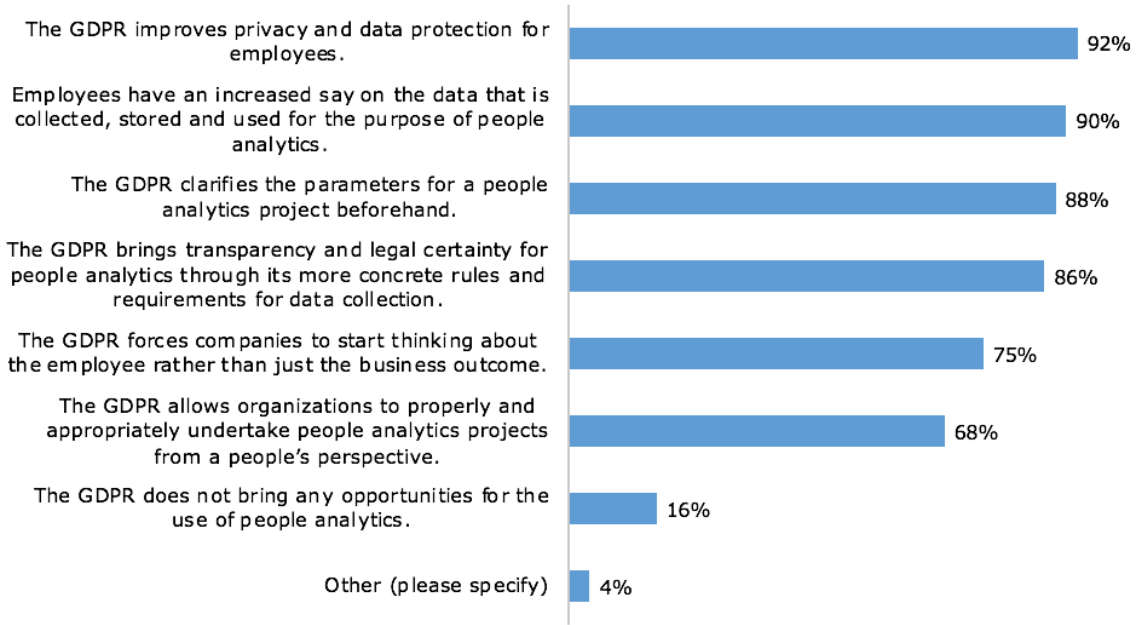
employees in people analytics projects. 88 percent expect the GDPR to clarify the parameters for people analytics projects up front, 75 percent agree that the GDPR forces organisations to start thinking about the employee instead of just the business outcome and 68 percent think the GDPR allows organisation to properly and appropriately undertake people analytics from the perspective of the employee. The fact that only 16 percent of the people analytics practitioners anticipate the GDPR to not bring any benefits for employees further confirms these findings. In case people analytics practitioners anticipated other benefits for employees not listed, the response option 'Other, please specify' was provided. However, no respondent made use of it.

Figure 1: The extent to which people analytics practitioners are informed about the new GDPR requirements and obligations.



Source: Survey on GDPR and People Analytics, May 2018, N=25

Figure 2: Anticipated implications of the GDPR for employees.



Source: Survey EU General Data Protection Regulation, May 2018, N=25

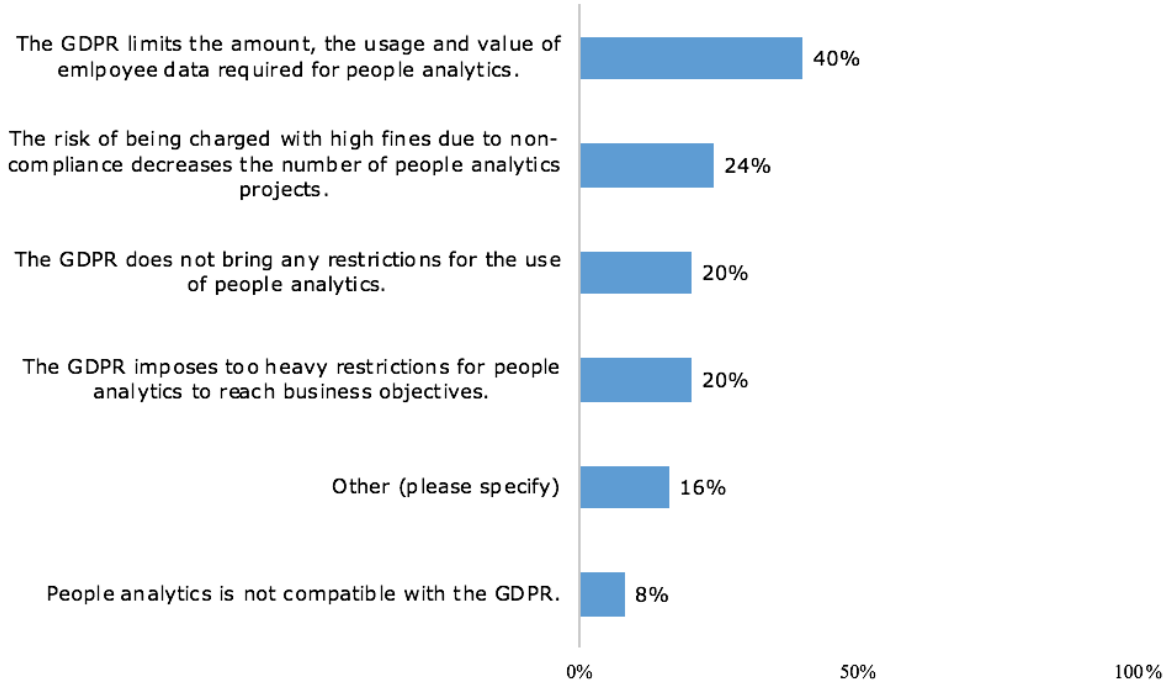
Following the high accordance of the results of the survey conducted with people analytics practitioners and the findings based on the interviews with experts in people analytics and the academic literature, the hypothesis *the GDPR is expected to improve the control of employees over their personal data and their overall influence in people analytics projects (H1)* can be supported. Since employees are expected to have control over their personal data by being able to grant or restrict organisations the access to their personal data, it can be concluded that the GDPR is also expected to secure the informational privacy of employees from the perspective of the control theory.

The survey further measured how people analytics practitioners value data protection compared to business outcome. On a scale of 1 (only business outcome) to 10 (only data protection), people analytics practitioners indicated that they value business outcome and data protection in their organisation on average 5.84. This average demonstrates a slight tendency of people analytics practitioners towards data protection. Furthermore, people analytics practitioners were requested to rate the statement 'Data privacy will be an influential factor shaping the future of people analytics', which 64 percent of the people analytics practitioners agreed to, and 12 percent strongly agreed to. These results further confirm that data protection of employees will increasingly be considered by people analytics practitioners.

Once established that the GDPR is anticipated to encourage the role of employees, the question arises how the GDPR can be expected to affect organisations using people analytics. Banjeree (2018) claims that privacy protection in the digital age does not directly imply that data should not be collected, stored or used, but should guarantee that data can only be used once consent and legitimate purposes are given. However, following the preliminary analysis, the GDPR is expected to restrict organisations to conduct people analytics. Figure 3 shows which restrictions or risks the people analytics practitioners expect the GDPR to bring for organisations. Strikingly, it reveals that overall only a few people analytics practitioners agree that the GDPR will restrict or carry risks for organisations using people analytics. Moreover, only eight percent of the people analytics practitioners think that people analytics is incompatible with the GDPR and therefore Hintze and LaFever's (2017) argumentation cannot be confirmed. A few of the people analytics practitioners (40 percent) expect the GDPR to limit the amount, the usage and value of employee data required for people analytics. Even less (25 percent) think the risk to receive high fines due to non-compliance decreases the number of people analytics projects or expect the GDPR to impose too heavy restrictions for organisations using people analytics to achieve business objectives (20 percent).

However, only 20 percent expect the GDPR not to bring any restrictions for organisations. Hence, these results still suggest that there are a few people analytics practitioners who think the GDPR brings restrictions and risks for organisations using people analytics. Similar to the previous question, a response section 'Other, please specify' was provided, which again no one selected. Comparing the results of the survey with the findings of the preliminary analysis, it can be concluded that they do not clearly correspond. Thus, the hypothesis that *the GDPR is expected to restrict organisations to conduct people analytics (H2)* cannot distinctly be supported and is thus rejected.

Figure 3: Anticipated implications of the GDPR for organisations using people analytics.



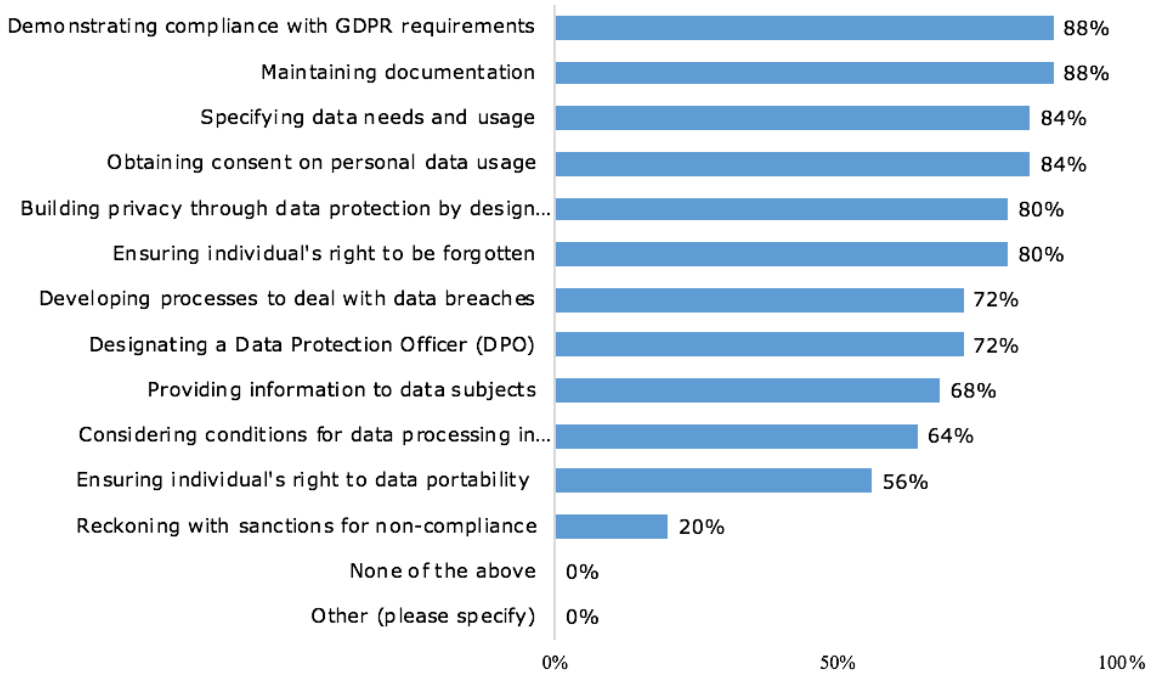
Source: Survey EU General Data Protection Regulation, May 2018, N=25

The people analytics practitioners were additionally asked to indicate their overall opinion on the GDPR, which 40 percent indicated as very valuable and 50 percent as somewhat valuable. It can be argued that these results show that people analytics practitioners rather welcome the GDPR instead of expecting risks or restrictions for organisations conducting people analytics. Thus, whether the GDPR can be expected to restrict organisations to conduct people analytics remains unclear.

The extent to which organisations comply with the GDPR influences anticipated implications of the GDPR for organisations using people analytics. However, one of the anticipated risks discussed in the preliminary analysis concerns the non-compliance of organisations. Although the GDPR introduces new specific and clarified requirements and obligations, it does not provide specific guidelines (Tikkinen-Piri et al., 2018). The fact that organisations need to determine solutions for themselves could serve as a reason for the anticipated concern. According to studies in 2013, 2014 and 2015, less than half of the companies were aware of the GDPR changes (Tikkinen-Piri et al., 2018). However, a research study conducted in 2016 claims that 48 percent of the participating organisations were preparing for the GDPR and 91 percent of the organisations were at the very least worried about non-compliance (Tankard, 2016).

Two years later, at the end of the transition period and shortly before the GDPR will be enforced, the survey tested which of the GDPR requirements identified by Tikkinen-Piri et al. (2018) organisations using people analytics have prepared for and comply with. Overall, Figure 4 shows that organisations have prepared for and comply with the majority of the twelve aspects but to a varying extent. Most of the people analytics practitioners (88 percent) indicate that their organisation has prepared for and complies with demonstrating compliance with GDPR requirements and maintaining documentation. The fewest organisations have prepared for and expect sanctions for non-compliance (20 percent). The rest of the results suggest that the majority of the GDPR requirements have been addressed by more than 50 percent of the organisations using people analytics.

Figure 4: The extent to which organisations using people analytics have prepared for and comply with GDPR requirements and obligations identified by Tikkinen-Piri et al. (2018).



Source: Survey on GDPR and People Analytics, May 2018, N=25

However, not all twelve aspects have been prepared for and are complied with by all organisations. These organisations should improve their preparation and compliance by May 25, 2018. Moreover, based on the results it can be argued that some GDPR requirements and obligations, for instance, maintaining documentation, seem to require less effort to prepare for and comply with than other aspects such as ensuring individuals' right to data portability or reckoning with sanctions for non-compliance. Following the results, it can be concluded that organisations using people analytics have not yet fully prepared for and comply with the GDPR requirements but are assumed to be in the process of it. However, at this point, it cannot be concluded whether the risk of non-compliance can be confirmed.

The organisations' current state of compliance was further examined by measuring the overall alignment with the GDPR and the concern of non-compliance of organisations. The results show a similar picture. On average people analytics practitioners think their organisation is 7.24 out of 10 (fully aligned) aligned with the GDPR and are only 3.84 out of 10 (extremely worried) worried that their organisation is not compliant with the GDPR. These results confirm the assumption that organisations using people analytics still review and revise their current organisational and technical privacy protection measures and develop new policies to ensure their alignment with the GDPR.

7. Conclusion

The objective of this study was to analyse the GDPR in the context of people analytics. Understanding how the GDPR can be expected to affect organisations using people analytics and their employees has high relevance for employees to examine whether the GDPR responds to their privacy concerns and for organisations to investigate whether they are still able to conduct people analytics. This study approached the research in a two-step analysis. By firstly analysing interviews conducted with experts in people analytics and secondary literature, hypotheses were established, which were secondly analysed based on a survey conducted with people analytics practitioners. Two general conclusions can be derived from this analysis.

Firstly, the GDPR is expected to improve the control of employees over their personal data and their overall influence in people analytics projects. The control theory further enables to conclude that because the employees are anticipated to gain more control to restrict or grant organisations access to their personal data, their informational privacy is ensured. Moreover, data protection will increasingly be considered by people analytics practitioners.

Secondly, it could not be concluded whether the GDPR is expected to restrict organisations to conduct people analytics. While a few expect this to happen, it overall remains unclear. Furthermore, whether non-compliance of organisations using people analytics demonstrates a potential risk, could not be evaluated at this stage. However, based on the overall tendency it can be assumed that organisations using people analytics are in the process to prepare for the GDPR changes, which implies the GDPR will have implications on these organisations.

Since the analysis of anticipated implications for organisations using people analytics did not produce explicit results, further research needs to be conducted to assess whether the GDPR is expected to restrict or carry risks for organisations using people analytics or whether the GDPR is anticipated to affect organisations using people analytics in a different way. Moreover, further research could replicate this research at a later point of time, now that the GDPR came into force. The results could be compared to see whether the anticipated implications of the GDPR examined in this research prove true. Moreover, it could be analysed whether organisations now comply with the GDPR requirements and obligations or whether they are charged with fines for non-compliance.

It needs to be noted that this research may suffer from few limitations. First of all, the number of 25 participants in the survey is rather small, which could decrease the validity of the survey's results. The limited number of responses further rendered it impossible to limit the case selection. The demographic information varied to the extent that it could not be compared. The limited number of respondents could be explained by the fact that the people analytics practitioners did not see any added value in filling in the survey. Moreover, the fact that employees were not included in the survey nor interviewed serves as another limitation. This research set the focus on experts in people analytics and practitioners, but further research could include employees. This research was conducted in light of the EU's overall need to balance privacy and data protection and promoting data sharing to encourage data innovation and progressions such as people analytics. While this research clearly demonstrates how the GDPR is expected to strengthen privacy and data protection of employees, it does not reveal whether people analytics can be still promoted or is restricted.