Implementing GDPR in the Charity Sector: A Case Study

Jane Henriksen-Bulmer, Shamal Faily, Sheridan Jeary

Implementing GDPR in the Charity Sector: A Case Study

Jane Henriksen-Bulmer[1], Shamal Faily[1], and Sheridan Jeary[1]

Bournemouth University, Poole, UK
{jhenriksenbulmer,sfaily,sjeary}@bournemouth.ac.uk

Abstract. Due to their organisational characteristics, many charities are poorly prepared for the General Data Protection Regulation (GDPR). We present an exemplar process for implementing GDPR and the DPIA Data Wheel, a DPIA framework devised as part of the case study, that accounts for these characteristics. We validate this process and framework by conducting a GDPR implementation with a charity that works with vulnerable adults. This charity processes both special category (*sensitive*) and personally identifiable data. This GDPR implementation was conducted and devised for the charity sector, but can be equally applied in any organisation that need to implement GDPR or conduct DPIAs.

Keywords: Privacy · Case Study · General Data Protection Regulation · GDPR · Contextual Integrity · Privacy Risk · Data Protection Impact Assessment · DPIA.

1 Introduction

The General Data Protection Regulation (GDPR) is the European Union's (EU) new Data Protection Regulation that came into effect on 25th May 2018 [9]. While GDPR affects all organisations, it has particular implications for small to medium enterprises (SMEs) and charities, who, like many other organisations, collect and process personal and/or "special category" (*sensitive*) data, as these organisations often work within financial and resource restraints and therefore, may lack the expertise to fully understand how best to interpret and implement the changes brought in by GDPR. In the UK, the Data Protection Act 1998 (DPA) has been incorporated into UK law through the Data Protection Act 2018 [31], which is in line with GDPR.

GDPR imposes several new obligations on organisations; these include extending the scope and breadth of what data is classed as personal, more rights for individuals in relation to their data; a requirement for organisations to understand and document their data holdings; justify why they collect each piece of data and record the lawful basis for processing data. GDPR also introduces data protection by design and default (DPbDD) and a requirement for organisations to demonstrate compliance to the relevant authorities if challenged.

Privacy protection in practice must be meaningful to be effective [1]. Privacy has to be implemented to not only account for legal requirements but also the

context within which privacy protection is required, including looking at the specific sector or industry an organisation works within. Thus, while GDPR may not necessarily require expert knowledge to implement, the requirements and obligations still require interpretation. Charities, like many organisations, find it difficult to fully understand when and how best to implement GDPR.

We present a case study that illustrates how charities and small & medium-sized enterprises (SMEs) can implement GDPR in an organised, step by step approach. As part of this we also present the DPIA Data Wheel: a Data Protection Impact Assessment (DPIA) framework for assessing what the privacy implications of processing data within the organisation are. There are no current solutions for implementing GDPR or carrying out DPIAs in this context. This work will, therefore, benefit any charity or SME dealing with vulnerable clients. Our approach builds on previous work using Nissenbaum's Contextual Integrity (CI) framework [21] to create a decision framework that assess privacy risks in Open Data [12], and expands on this to support the GDPR implementation and the DPIA framework.

The rest of the paper is structured as follows. We begin by providing an overview of the changes brought in by GDPR in Section 2 . This is followed by a brief review of risk assessment (Section 2.1), before discussing privacy, data privacy and how Contextual Integrity can assist in assessing privacy risks in Section 3. This is followed by details of the case study in Section 4, outlining the action intervention for implementing GDPR and creating the DPIA framework aimed at SMEs and the charity sector. Finally, we conclude and outline directions for future work in Section 5.

2 General Data Protection Regulation (GDPR)

GDPR Article 5 sets out 6 Principles (P): (P1) *Lawfulness* i.e. determining and defining the lawful basis for processing the data; *Fairness* i.e. processing the data fairly with data subjects interest in mind; and *Transparency* i.e. specifying the data to be collected and why, while keeping the data subject(s) informed of how their data will be used. (P2); *Purpose Limitation* i.e. collecting only relevant and necessary data, and processing such data fairly with data subjects interest in mind. (P3) *Data Minimisation* i.e. collecting minimum data, and only collecting data necessary for the specified purpose. (P4) *Accuracy* i.e. keeping the data up to date and correct. (P5) *Storage Limitation* i.e. retaining the data no longer than necessary, and (P6) *Integrity and Confidentiality* i.e. protecting, processing and storing the data securely, and ensuring data is protected from harm, unauthorised or unlawful access.

Data Protection Officers (DPOs) and/or the Data Controller ensure organisations implement appropriate technical or procedural measures to ensure and demonstrate compliance (GDPR, Article 24). To this end organisations must adopt a privacy first policy (DPbDD, GDPR, Article 25), maintain a record of processing activities (GDPR, Article 30), and implement appropriate security measures to protect the data (GDPR, Article 32). Under GDPR Article 35, any

processing likely to pose a high risk to the rights and freedoms of the data subject must be assessed. This obliges organisations to assess risks, not from an organisational perspective, but from the perspective of the data subject (the individual). This is the area that this study seeks to address.

2.1 Risk

GDPR asks that organisations must conduct DPIAs for any *high risk* processing activities. High risk processing refers to any large scale processing of personal data. This includes tracking, monitoring, profiling, implementing new technologies, or processing genetic, biometric or special category data (e.g. data relating to health or criminal records) on a large scale (GDPR, Article 35). Processing refers to: *"any operation or set of operations which is performed on personal data or on sets of personal data ... such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available"* (GDPR, Article 4(2)). The Data Subject is the person whose data is being processed, while the Data Controller is the legal entity responsible for making decisions about how the data is processed, this includes any: *"natural or legal person, public authority, agency or other body"* (GDPR, Article 4(7)). Where a third-party processes the data on behalf of the Data Controller, they are referred to as the Data Processor (GDPR, Article 4(8)) or, if a partner organisation jointly manages the data with the Data Controller, they may be the Joint Data Controller.

Conducting a DPIA involves assessing privacy risk. Assessing risk is an integral part of business processes, and helps organisations make informed decisions. However, for privacy, this is usually an extension of assessing security risk. Organisations can use several internationally recognised frameworks for conducting structured risk assessments such as the National Institute of Standards and Technology (NIST) risk framework [22], [23], and the International Office of Standardisation's (ISO) [4], [11] and [16]. However, these frameworks focus on organisational risk, and don't satisfy GDPR's requirement for assessing risks to the data subject (the individual).

3 Privacy and Contextual Integrity

Our right to privacy as a concept is not a new idea, as early as 1890, Warren and Brandeis discussed *the right to be let alone* [29], while Westin framed privacy from the perspective of the right to control personal information and, in doing so, recognised the content dependent value of information [30]. This idea has since been elaborated and expanded upon. Some refer to privacy as a fluid concept with blurred boundaries [24] or, a contested concept with many facets [18], depending on the context within which it is viewed [28]. Thus, privacy is subjective; every individual has their own view of what privacy is and 'tolerance' (values) or norms of what they consider 'normal' or 'acceptable' when it comes to their privacy [21].

Context has been previously considered as part of a privacy assessment. For example, Solove [28] divides privacy into four broad groups: *Invasions*, *Information collection*, *Information processing*, and *Dissemination*, while Bamberger and Mulligan [18] divide privacy into "five meta-dimensions of theory, protection, harm, provision and scope", sub-divided into 14 sub-dimensions that consider privacy in terms of risk or potential harm. This is akin to security threat modelling, which could assist software design teams in aligning threat modelling with privacy. Ultimately, privacy must be integrated into organisational decision making and thus built into corporate practice [1], which GDPR seeks to achieve through the introduction of DPbDD.

These frameworks consider context but, context is not just about how organisations perceive data privacy. Perceptions and behaviours help people shape what privacy is to them and therefore, when it comes to information and data privacy, their values and norms influence how they perceive data privacy [20]. This can be observed by the choices individuals make about whether or not to share information, how they share information, and why. Some are comfortable sharing very personal details on social media, others are more selective about what they share, and others avoid sharing any information at all. Therefore, there is a difference between what a person chooses to share about themselves and what is shared by others about them i.e. WHO is doing the sharing [20]. Someone may accept their friend sharing their photo within a social circle on Facebook, but not so, if that same photo was shared with the government or their employer given the possible unintended consequences [26,28].

Contextual Integrity (CI) [21] accounts for these previously described contextual nuances. CI considers privacy in terms of data flows, proposing that data privacy should be concerned with how data flows between stakeholders ("transmission principles"), combined with the context within which the data is transmitted. This means that, when it comes to data privacy and how personal data is processed by government departments and organisations, they should primarily be concerned with the individual's "right to an appropriate flow of information" [21]. Thus, CI encompasses all the aspects discussed by Solove [28] and Mulligan et al. [18] but frames these nicely within a theoretical framework devised for decision making and assessing privacy risks in data.

CI assesses privacy risks through three key elements: *Explanation* looks at the current status quo, what the prevailing context is, and how data is used, transmitted, and by whom, *Evaluation* assesses how the data will be transmitted in the proposed new flow, by whom and how this changes the context, and *Prescription* decides if a decision can be made about whether or not the changed flow increase or decrease the privacy risks. Within each of these key elements, the risks are evaluated by looking at privacy from four perspectives: *Actors* (the data- subject(s), sender(s) and receiver(s)), *Attributes* (the individual data items), the *Transmission Principles* (how data is distributed and shared), and the *Context*, i.e. by considering the established norms and values of the actors and society and how these might influence or affect the information flows. For example, actors should be evaluated in relation to their social and job role, the

activities of each role, and the values and norms expected of that role. There may also be contrasting duties, prerogatives or obligations associated with one of those roles that could undermine the relationship between the data subject and the person processing the data. Thus, like [18], CI views privacy through a risk lens, but focuses on decision making rather than threats and protection.

CI has been used in theoretical discussion about its applicability to a particular scenario or situation [6], although there have been some attempts to consider how CI might be applied in practice. For example, CI has been used to consider appropriate access controls for information flows in system design [2], how attaching tags in message headers can preserve privacy [17], and whether particular practices or sites provide sufficient privacy protection [10,27].

CI has also been used to inform decision making around high level privacy goals for a user community [7], and assessing privacy risks associated with publishing open data [12], which found that organisations consider the data and the attributes when assessing privacy, but fail to take account of the context within which the data is processed. However, by applying CI and also considering the context, more informed decisions could help facilitate the publication decisions. We extended on this work in a case study where we sought to incorporate CI into a DPIA as part of a GDPR implementation process, this is discussed in the next section.

4 Case Study

In this section, we present a case study of an exemplar approach to GDPR implementation in the Charity Sector. The implementation of GDPR will also incorporate the design and creation of a DPIA framework, the DPIA Data Wheel, aimed at this sector and SMEs.

4.1 Background

Most charities rely on public generosity for funding and in-kind support from volunteers to function, with many struggling to raise enough funding to meet all the objectives for their cause. Much work is conducted by volunteers meaning that, even though a charity may collect and manage personal data, they often lack the resources and expertise to assess themselves against legal regulations.

The UK Information Commissioners Office (ICO) has issued some guidance on GDPR to help organisations implement the regulation, but this is so general as to be applicable to all types of organisations [13]. No sector specific guidance is available for the charitable sector, despite requests from the sector for more specific guidelines to be produced [15]. We, therefore, decided this sector would benefit from some assistance and chose to work with a local charity ('the Charity') to provide an exemplar approach to GDPR implementation.

The Charity supports those suffering from addiction and substance misuse. It collects personal data from clients to provide them with the care and assistance for dealing with or overcoming their problems. The Charity also needs to ensure

data collection and processing satisfies data protection laws, and they rely on several procedures to ensure all processes comply with requirements laid down by legislation such as GDPR and the Care Act 2014. The Charity shares some of the data collected from and about clients with external stakeholders. These may be clinicians and professionals who work with the charity and their clients in providing treatment and advice, or Governing bodies they are legally obliged to share data with, e.g. the Care Quality Commission (CQC) that regulate health and social care in England [5] or the National Drug Evidence Centre (NDEC) that collates statistics on adult addiction users and their treatment [19].

4.2 Approach

We worked with two managers and 29 staff and volunteers who work for the Charity. The case study was conducted over three months and incorporated three staff training sessions and a workshop for a group of 40 other local charities to disseminate the results and evaluate the DPIA Data Wheel. Ethics approval for this case study was sought and granted from the University Ethics Committee.

The research questions (RQ) we asked were: *what data holdings does the Charity have, where and how are these handled currently and to what extent do these comply with GDPR standards?* (RQ1); *what processes does the organisation need to put in place for effective GDPR implementation to demonstrate GDPR compliance?* (RQ2); and *how can the organisation ensure they have in place appropriate processes conducting DPIAs going forward?* (RQ3). The hypothesis supporting these questions and the full methodology can be found at [1].

This project was conducted as an action intervention case study [32], with the unit of analysis being the the Charity as GDPR affects all aspects of the organisational processing of data. The first step was to make a detailed GDPR implementation plan evaluating the Charity's readiness, and its ability to achieve DPbDD and demonstrate GDPR compliance to the ICO. The case study was conducted in four phases, each will be described in more detail in the below sub-sections.

4.3 Phase 1 - Data Holdings

We decided that a draft data register would answer RQ1 and help the Charity achieve DPbDD. Therefore, the first step entailed understanding what data the Charity held and how this was processed. This would establish a baseline of what data is collected and how this data is processed within the Charity.

Two parallel pieces of work were carried out: establishing what forms were used within the Charity to collect data, and collecting staff stories. Storytelling as a research method involves collecting narratives or stories to understand people, their actions and ideas. For this study, this would entail staff recounting how they process data as part of their working day using a user story methodology[3,25].

[1] `https://github.com/JaneHB/DPIA-CS-Protocol`

To determine what forms were used within the Charity, the project started with a meeting to discover more about where the Charity were with their GDPR implementation and establish what data was collected and processed within the Charity. This was a very informative meeting which formed the basis upon which the rest of the project was based. It also became evident that the majority of data collection and processing was paper based, securely stored in locked cabinets when not in use. As part of this meeting, copies of the various forms in use as part of the daily operations of the Charity were provided to the research team.

These forms were used as the basis for creating a draft data register containing details of each attribute (individual data item) collected and categorising these based on data sensitivity. This draft register was then further elaborated upon with the information obtained from the parallel piece of work, collecting staff stories.

To collect the staff stories, a spreadsheet was created with 9 columns to capture details of who staff communicate with, what data is communicated, how the communication takes place (e.g. paper or electronic), the regularity of the communication, how long each communication takes, how demanding the staff member finds each communication to be, and whether the communication interferes with or interrupts other duties. The questions asked can be found in the protocol (see [2]). These spreadsheets were circulated to all staff, with 21 staff members respondents, working in eleven different roles. The gender of the respondents was well balanced with approximately half of the respondents being male (9) and half female (10), two respondents chose not to provide gender details.

Some staff completed their stories with few words using one line sentences while others were more descriptive in their stories. Therefore, once the staff stories had been collated, the completed staff stories were returned with an additional column containing questions that sought clarification on different aspects of the staff stories. For example, different staff members referred to different forms using alternate names than those initially collected making it necessary to clarify terminology or confirm which terminology related to each form.

4.4 Phase 2 - Analysis of data holdings

The staff stories were analysed to update the draft data register, confirm the list of forms used within the Charity, and gain an overview of how the data travels (the data flows) both internally and externally. From this, it became clear that there were more forms used than originally collected as part of the initial meeting. Consequently, a second meeting was scheduled to update the list of forms, and seek clarification on some of the terminology used; various forms were referred to in different ways by different staff members. At this second meeting, the research team was granted access to the form templates used within the Charity.

[2] Ibid 1

Life of the form Comparing the template forms collected and the staff stories showed the client assessment and care plan forms were the forms containing personal data that was processed most regularly. Both were living documents that included detailed personal information. These included a full medical history (mental and physical), details of a client's social, personal and cultural background, and a list of historic and current professionals responsible or involved with their care. Both documents form part of the contract between the client and the Charity.

These two forms were chosen to capture the data journey through the "life of the form" exercise. This data collection involved another spreadsheet (the "life of the form") devised to investigate in more detail how the data travels, i.e. how these forms are used, transmitted or shared both internally within the Charity and externally with other stakeholders. This spreadsheet asked a series of questions about the journeys the data might take such as where the form that collects the data was born (see [3] for full list).

A column was created within the spreadsheet for each sub-form. Creating multiple columns would allow separate elements to go on different journeys. For example, a page or sub-form may be removed or shared for specific purposes such as faxing to external key professional staff involved in the care of the client, could be captured as part of one of the journeys. The spreadsheet supported up to 10 journeys for each sub-form. The life of the form spreadsheets for the Care Plan and Client Assessment were sent to the CEO and the manager of one of the Charity's houses to be completed with details of how the data travels during its lifecycle.

Analysis The staff stories were compared with the forms to identify any missing forms, and establish patterns of data flow. This revealed that records pertaining to the client's medication and the client register were the most frequently referred to documents. Moreover, various methods of communication between staff and other stakeholders were mentioned as part of the staff stories. This information was then compared to the completed life of the form spreadsheets to provide a more detailed overview of the data, how it was used and the "journey" each form went on during its life cycle.

This analysis showed that the Charity collect a variety of personal or special category data from their clients that require a legal basis for processing under both Article 6 and Article 9 of GDPR. This included details relating to health, religion and beliefs. The analysis also highlighted a number of common processes and procedures undertaken by staff as part of their daily work, or the form's journey. These were broken down into data relating to clients and data relating to staff and data processing processes.

Master Data Register This information was then used to turn the draft data register into a Master Data Register (MDR) providing details of all the Charity's data holdings. The data included within the MDR was informed by the

[3] Ibid 1

draft register, the information gleaned from the staff stories and the list of forms downloaded from the second meeting, listing all the individual attributes from each form and categorising these based on level of sensitivity of the data. Personally identifiable data was classed as personal data in accordance with GDPR Article 6, while most of the data collected and classed as sensitive was classed as "special category" data in accordance with GDPR Article 9. The initial data categorisation was based on "best guess" from the information available. These categories were then evaluated by the Charity CEO who verified or changed each of the categories according to the Charity's perspective. The MDR also sought to include several other pieces of information including details of the Data Controller, a justification for collecting each piece of data, details of the processing being carried out, how the data will be stored, and the storage period etc. [4].

The final MDR contained 997 individual data items, categorised according to data sensitivity and justified based on relevant legislation or contractual obligations to facilitate the clients' (*data subjects*) treatment needs. Creating this MDR answered RQ1 and provided the Charity with their starting point towards demonstrating compliance with the obligation to keep "records of processing activities" (GDPR, Article 30).

4.5 Phase 3 - GDPR Process Guidance

Phase three sought to answer RQ2, and involved assessing existing processes and practices to determine how these could be revised to ensure GDPR compliance. The work in this phase centred on reviewing policies and protocols and preparing the supporting documentation and processes necessary for the Charity to demonstrate GDPR compliance. The Charity's privacy policies were reviewed and revised, together with the process for obtaining consent from Clients; and a process for responding to data subject requests for access, erasure and data portability was also created.

Privacy Policies and Data Subjects' Rights The existing privacy policy given to clients by the Charity was in line with Data Protection Act 1998, but failed to meet the requirement of expressing clearly, in plain language, what data the Charity collect from clients and how this is used. Therefore, a new policy was devised to meet these requirements. This was presented in plain language and includes details of what data is collected, how the data is collected and used, who the data is shared with, how the data is safeguarded, the timeframe for storing the data and details of the data subjects rights in relation to their data. To compliment the new policies, the Charity agreed to create a protocol for dealing with and responding to clients seeking to invoke their rights (e.g. requests for access, erasure and data portability etc.). This ensured a thorough, repeatable procedure was in place to deal with a data subject (client) invoking their rights under GDPR. The privacy policy for staff was also updated to ensure staff are fully aware of their obligations under GDPR.

[4] Ibid 1

Consent The issue of consent is a potential problem for the Charity. It works with vulnerable adults who may initially give consent to processing, but later withdraw their consent or even claim consent was not freely given. For example, a client may claim that they were not capable of giving informed consent at the time or claim they lacked sufficient mental capacity to freely give consent. Thus, there is potential that the Charity's clients (or someone else on their behalf) may argue that consent was not freely given, because there is a power imbalance between the client ("the data subject") and the Charity (as "the data controller") providing the client with treatment and thus, exercising a level of control over the clients and their actions while under their care (GDPR, Article 7). To address this, a meeting was convened to understand precisely what consent was collected from clients (data subjects), how this was collected and used, and what procedures allowed clients to withdraw their consent. Following this meeting and careful study of the legislation, the solution was providing more clarity for the legal basis for processing the data in the first place.

The Charity only processes data to provide effective treatment to their clients as required under the Care Act 2014 (CA). Although the Charity ensures informed consent is obtained from all clients, this is not the main legal grounds for processing the data. When enrolling for treatment, clients complete a "Client Assessment" and "Care Plan". Both documents subsequently form part of the contract between clients and the Charity. The data collected is gathered to satisfy a legal requirement to assess the clients needs prior to and, as part of, providing treatment to vulnerable adults (CA, s. 9), making it necessary for the Charity to provide effective treatment; they cannot help clients without the full history of their addiction and the surrounding circumstances.

The Charity can, therefore argue that the processing is necessary for compliance with a legal obligation (GDPR, Article 6(1c)), or the primary legal basis for processing the date is contractual (GDPR, Article 6(1b)) because they cannot perform their work without this information. However, this does not mean that consent is not still required; some aspects of sharing the data may not be required to perform the contract. For example, family members may wish to be kept informed of how the client responds to treatment, which is not a prerequisite requirement for providing treatment. Therefore, for those aspects, informed consent remains required from the client for this type of secondary sharing of the data (GDPR, Article 7(2)). This means the Charity remains compliant provided clear instructions are given that are "clearly distinguishable" from other types of data processing, and provide an easy means for amending or withdrawing consent settings. To this end, the Charity, as part of the contract, would obtain granular informed consent for who they may or may not divulge information to from the client. In addition, a granular "withdraw consent" section was added to the consent form, allowing clients to withdraw easily.

In addition staff training was arranged to inform staff about GDPR, consent and the new protocols, e.g. what these mean for the organisation, for them as staff, and as individuals. The training sessions were designed to make staff think about how they process data as part of their daily work. The training was

positively received with one participant commenting; *I will be mindful and start to prompt colleagues around having data around* (P23), suggesting this exercise is likely to positively impact on their behaviour in dealing with data in future.

4.6 Phase 4 - The DPIA Data Wheel

The final phase of the project sought to answer RQ3 by creating a DPIA process for assessing privacy risks. The DPIA was devised based on previous work on assessing privacy risk for open data [12], GDPR, and guidance provided by the ICO on how to conduct DPIAs [14]. The resulting DPIA framework, named "the DPIA Data Wheel", is a step-by-step guide that takes assessors through the process of conducting a DPIA (see Figure 1, and [5]). The DPIA Data Wheel incorporates questions about the *prevailing* and *surrounding* context to ensure the wider implications of data processing are considered. Moreover, by including the Data Register and the life of the form questionnaire devised and used in Phases 1 and 2, we have facilitated the gathering of comprehensive background information about the data, the actors and the transmission principles (*data flows*) to inform the risk assessment in the Data Wheel. This provides a mechanism that any organisation can use for establishing their own data register and detailed data journeys, thereby acting as a starting point for their own GDPR implementation.

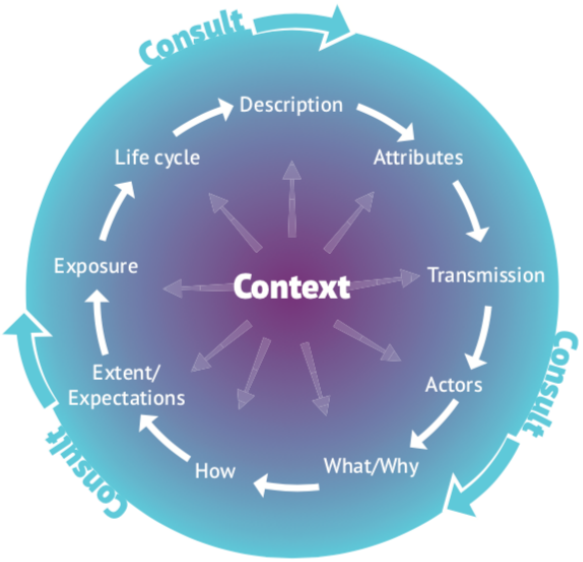

Fig. 1. DPIA Data Wheel

[5] Ibid 1

The DPIA Data Wheel asks a series of questions relating to the data devised to provide a full overview of the system, process or project being assessed. The full DPIA Data Wheel is presented in a spreadsheet consisting of 5 tabs, the last containing the various drop-down lists within the spreadsheet. For information purposes, this has been left so practitioners can view this information. These are:

Tab 1: Need for a DPIA This is the starting point for conducting the DPIA, and consists of a short assessment to help the practitioner determine whether or not a DPIA is required for the system, project or process under review.

Tab 2: Data Wheel Where a DPIA is required, the Data Wheel is the privacy risk assessment for the process, system or project. As part of this, the DATA part of the Wheel provides the *explanation* [21], while the WHEEL forms the beginning of the risk assessment (the *evaluation*). Practitioners are asked to consider different aspects of the process, system or project including what data they plan to capture (*the "data"*), the people who will process the data (*the "actors"*) and the context within which data is processed (thereby embedding the *context* element of *"CI"*);

Tab 3: Data Register This was derived from the draft data register created as part of Phase 1. Practitioners are asked to provide more specific and granular details about the data attributes (individual data items) that they plan to process (*the "data"*). The information gathered here is intended for use to compliment and help inform the risk assessment on Tab 2. It was designed to form part of the organisation's Master Data Register, thereby helping them maintain an accurate overview of the organisation's data holdings;

Tab 4: Life of the form The questions here were derived from the "life of the form" part of the project. It was included to make practitioners think about how the data travels within their organisation. (*the "transmission principles"*). By considering the 'journey' the data within the system, project or process is likely to take during its lifetime, practitioners will be able to glean valuable insight into where there may be potential risks that will need to be mitigated against;

Tab 5: List This contains list of all the drop-down menus that form part of the assessment on the other tabs.

The final aspect of the DPIA framework is the "consult" element. This element is not present in the DPIA Data Wheel spreadsheet as this involves ensuring that all relevant stakeholders with a potential interest or input into the process, system or project are consulted on the privacy risks as far as is possible. In the case study, this element was completed through the staff training sessions where the risks identified by management as part of completing the DPIA framework. This served two purposes. First, it allowed the research team to evaluate the effectiveness of the DPIA Data Wheel. Second, it helped avoid "resistance to change", which is a common reaction of staff when any form of change is introduced within an organisation [8]. This is discussed in the next section.

Evaluating the DPIA Framework To evaluate the DPIA Framework, a DPIA Data Wheel spreadsheet was created for the "Care Plan" and "Client Assessment". On each DPIA, the Data Register and the Life of the Form tabs were pre-populated with the information provided as part of Phase 1 and 2, i.e. the list of attributes collated from the staff stories and the forms provided that the Charity use and the completed life of the form answers that the CEO and House Manager had provided.

The completed DPIA was evaluated in three ways First, by the CEO and the House Manager, who reviewed the DPIA Data Wheel, the Data Register and the Risk Register. Second, as part of the staff training session, the Risk Register was reviewed and evaluated with further risks added. Third, the DPIA Data Wheel was reviewed as part of a workshop where delegates from 40 local charities reviewed the Data Wheel and the Risk Register at an interactive workshop. As well as enabling the evaluation of the DPIA Data Wheel, it also enabled the final "consult" element of the DPIA framework to be achieved by taking the evaluation to stakeholders.

Following the first evaluation, several changes were made to the DPIA framework. Some questions were reworded slightly in the Data Wheel; one question was removed as a duplicate, and another added. In the Data Register, more columns were added for inputting justifications as one was not always sufficient. There can be more than one reason for why a particular attribute is collected, and the Charity wanted to capture these to strengthen their case for justification.

The second evaluation took place during three staff training sessions. These informed staff of the changes introduced by GDPR and provided consultation on the risks identified by senior staff when completing the DPIA Data Wheel. These sessions served as part of the DPIA consultation accounting for internal stakeholders, and resulted in several additional risks being identified that had not been included in the initial completion of the DPIA framework.

In the third evaluation, a group of industry or sector peers served as an external body of stakeholders in reviewing the DPIA Data Wheel. At the workshop, delegates were divided into four groups with each group reviewing the same DPIA Data Wheel. This produced a series of additional risks that had not been included in previous evaluations. Some were generic threats that were relevant to the Charity, such as failure to lock storage cabinets holding data. Others, such as the risk of not informing trustees of a breach, failure to delete data, or insider threat by staff, could be applied more generally across the industry sector.

These sessions resulted in 88 different risks being identified and suggested mitigation strategies for each of these recorded. The staff participants particularly appreciated *the application to our work and potential risks* (P9), while one workshop participant commented that the workshop provided *thought provoking and practical information* (P33). Interestingly, in all of the evaluation sessions, all of the threats identified were related to the organisation and how they should safeguard data rather than to the data subjects themselves, despite the Risk Register specifically having separate columns for risks to be identified for the data subject as well as the organisation. In hindsight, this was to be expected

as all previous work and guidelines has concentrated on security and how to safeguard systems and processes. What it did show, however, is that more work is needed to educate practitioners on the need to separate privacy from the perspective of the data subject when assessing privacy risks. Future work will look at this element and how this can best be achieved.

5 Conclusion

In this paper we have answered RQ1 by creating a Master Data Register for the Charity and established how the data is transmitted through the life of the form exercise that recorded how the data travels during its lifecycle. For RQ2 we reviewed and revised the Charity's privacy policies, provided staff training on GDPR and the DPIA risk assessment and arranged for new protocols to be devised to facilitate dealing with data subjects invoking their rights under GDPR. Finally, in creating the DPIA Data Wheel, a standardised DPIA process based on CI, we answered RQ3. The main findings are that CI can be successfully applied to DPIAs and GDPR implementations, although more emphasis needs to be placed on the fact that risks should be assessed from the data subject's perspective rather than the organisation. However, our results do demonstrate how CI can be embedded into DPbDD and the DPIA process to provide the means for other charities and SMEs to be able to use the DPIA Data Wheel to assist in their own GDPR implementation and conduct comprehensive and repeatable DPIAs going forward.

This paper has provided three contributions. First, an exemplar model was presented to illustrate how SMEs and charitable organisations can implement GDPR. Second, we presented the DPIA Data Wheel: a repeatable DPIA framework that facilitates repeatable, consistent privacy risk assessments within an organisation. Finally, we demonstrated how CI can be used to facilitate practical decision making by incorporating the CI concepts into DPIAs.

Future work will examine how these concepts can be developed and strengthened to better guide SME and charity practitioners in assessing privacy risks from the individual's perspective. This in turn will help both SMEs and charities to better safeguard the data subject's privacy from the organisational viewpoint.

Acknowledgments

This work was funded by the Bournemouth University Charity Impact Funding scheme at Bournemouth University.

References

1. Bamberger, K.A., Mulligan, D.K.: Privacy on the Ground: Driving Corporate Behaviour in the United States and Europe. the MIT Press: Mssachusetts Institute of Technology, London: England (2015)

2. Barth, A., Anupam, D., Mitchell, J.C., Nissenbaum, H.F.: Privacy and contextual integrity: Framework and applications. In: 2006 Symposium on Security and Privacy [serial online]. vol. 2006, pp. 184–198. IEEE Xplore Digital Library, Ipswich, MA (2006). https://doi.org/10.1109/SP.2006.32, cited By 0
3. Bruner, J.S.: Actual minds, possible worlds. [electronic resource]. Cambridge, MA : Harvard University Press, 1986. (1986)
4. BS ISO 31000:2009: British standards document bs iso 31000:2009: Risk management. principles and guidelines. Tech. rep., British Standard and the International Organization for Standardization (ISO) (2009)
5. Care Quality Commission (CQC): Care quality commission. [online] (2018), `https://www.cqc.org.uk/`
6. Conley, A., Datta, A., Helen, N., Sharma, D.: Sustaining privacy and open justice in the transition to online court records: A multidisciplinary inquiry. Maryland Law Review **71**(3), 772 – 847 (2012)
7. Darakhshan, J., Shvartzshnaider, Y., Latonero, M.: It takes a village: A community based participatory framework for privacy design. 2018 IEEE European Symposium on Security and Privacy Workshops, Security and Privacy Workshops, 2018 IEEE European Symposium on, EUROSPW pp. 112–115 (2018)
8. Demirci, A.E.: Change-specific cynicism as a determinant of employee resistance to change. Is, Guc: The Journal of Industrial Relations and Human Resources **18**(4), 1 – 20 (2016)
9. European Parliament and the Council of Europe: General data protection regulation (gdpr). Regulation (EU) 2016/679 5419/1/16, European Parliament and the Council of Europe, Brussels (April 2016)
10. Grodzinsky, F.S., Tavani, H.T.: Privacy in "the cloud": Applying nissenbaum's theory of contextual integrity. SIGCAS Comput. Soc. **41**(1), 38–47 (2011)
11. Hall, D.C.: Making risk assessments more comparable and repeatable. Systems Engineering **14**(2), 173 – 179 (2011)
12. Henriksen-Bulmer, J., Faily, S.: Applying contextual integrity to open data publishing. In: Proceedings of the 31st British HCI Group Annual Conference on People and Computers: Digital Make Believe. British Computer Society (2017)
13. ICO: Preparing for the general data protection regulation (gdpr): 12 steps to take now. Tech. Rep. V2.0 20170525, Information Commissioner's Office (May 2017)
14. ICO: Data protection impact assessments (dpias). [online] (2018)
15. ICO: General data protection regulation (gdpr) faqs for charities. [online] (2018), `https://ico.org.uk/for-organisations/charity/charities-faqs/`
16. ISO/IEC 29100: BS ISO/IEC29100: Information technology — security techniques — privacy framework. Tech. rep., British Standard and the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (2011)
17. Krupa, Y., Vercouter, L.: Handling privacy as contextual integrity in decentralized virtual communities: The privacias framework. Web Intelligence and Agent Systems **10**(1), 105 – 116 (2012)
18. Mulligan, D.K., Koopman, C., Doty, N.: Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. Philosophical Transactions. Series A, Mathematical, Physical, And Engineering Sciences **374**(2083) (2016)
19. National Drug Evidence Centre: National drug treatment monitoring system (ndtms). [online] (2018)
20. Nissenbaum, H.: Privacy as contextual integrity. Washington Law Review **79**(1), 119–158 (2004)

21. Nissenbaum, H.F.: Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford Law Books, Stanford: California (2010)
22. NIST: Guide to protecting the confidentiality of personally identifiable information (pii). Tech. Rep. 800-122, National Institute of Standards and Technology (NIST); U.S. Department of Commerce (2010)
23. NIST: Guide for conducting risk assessments. Tech. Rep. SP 800-30, National Institute of Standards and Technology (NIST); U.S. Department of Commerce, US: Gaithersburg: MD (September 2012)
24. Palen, L., Dourish, P.: Unpacking 'privacy' for a networked world. CHI - CONFERENCE pp. 129 – 136 (2003)
25. Rooney, T., Lawlor, K., Rohan, E.: Telling tales: Storytelling as a methodological approach in research. Electronic Journal of Business Research Methods **14**(2), 147 – 156 (2016)
26. Sanchez Abril, P., Levin, A., Del Riego, A.: Blurred boundaries: Social media privacy and the twenty-first-century employee. American Business Law Journal **49**(1), 63–124 (2012)
27. Sar, R.K., Al-Saggaf, Y.: Contextual integrity's decision heuristic and the tracking by social network sites. Ethics and Information Technology **16**(1), 15 – 26 (2013)
28. Solove, D.J.: A taxonomy of privacy. University of Pennsylvania Law Review **154**(3), 477 – 564 (2006)
29. Warren, S.D., Brandeis, L.D.: The right to privacy. Harvard Law Review **IV**(5), 193–220 (Dec 1890)
30. Westin, A.F.: Science, privacy, and freedom: Issues and proposals for the 1970's. part i–the current impact of surveillance on privacy. Columbia Law Review **66**(6), 1003–1050 (1966)
31. www.parliament.uk: Data protection act 2018. [online] (May 2018)
32. Yin, R.K.: Case study research : design and methods. Los Angeles, California : SAGE, 2013. (2013)