electronics

MDPI

Article

Privacy Essentials

James Taylor, Jane Henriksen-Bulmer * and Cagatay Yucel

Department of Computing & Informatics, Bournemouth University, Fern Barrow, Poole BH12 5BB, UK; cyucel@bournemouth.ac.uk (C.Y.)
* Correspondence: jhenriksenbulmer@bournemouth.ac.uk

Abstract: Following a series of legislative changes around privacy over the past 25 years, this study highlights data protection regulations and the complexities of applying these frameworks. To address this, we created a privacy framework to guide organisations in what steps they need to undertake to achieve compliance with the UK GDPR, highlighting the existing privacy frameworks for best practice and the requirements from the Information Commissioners Office. We applied our framework to a UK charity sector; to account for the specific nuances that working in a charity brings, we worked closely with local charities to understand their requirements, and interviewed privacy experts to develop a framework that is readily accessible and provides genuine value. Feeding the results into our privacy framework, a decision tree artefact has been developed for compliance. The artefact has been tested against black-box tests, System Usability Tests and UX Honeycomb tests. Results show that Privacy Essentials! provides the foundation of a data protection management framework and offers organisations the catalyst to start, enhance, or even validate a solid and effective data privacy programme.

Keywords: data privacy; general data protection regulation; UK GDPR; compliance; privacy framework; charity; not for profit

check for updates

Citation: Taylor, J.; Henriksen-Bulmer, J.; Yucel, C. Privacy Essentials. *Electronics* **2024**, *13*, 2263. https://doi.org/10.3390/electronics13122263

Academic Editors: Lixin Wang, Jianhua Yang, Radhouane Chouchane and Linqiang Ge

Received: 30 April 2024
Revised: 3 June 2024
Accepted: 6 June 2024
Published: 9 June 2024

1. Introduction

We have observed an evolution of legislative changes regarding privacy with the Data Protection Act (1998), Freedom of Information Act (2000), EU ePrivacy Directive (2002), General Data Protection Regulation (2018), and UK Data Protection Act (2018) over the first quarter of the 2000s. This evolution reflects a collaborated effort to adapt legal frameworks to the challenges stemming from technological developments while increasing the complexity of the procedures surrounding personal data. This study underscores data protection regulations and the challenges of implementing these frameworks. To address these issues, we developed a privacy framework to assist organisations in taking the necessary steps to comply with the UK GDPR, highlighting the current best-practice privacy frameworks and the requirements set by the Information Commissioner's Office.

The UK is a generous nation with a long philanthropic tradition, donating a total of GBP 83 bn to more than 169 k registered charities in 2021. However, this also increases the potential for deliberate harm [1]. To demonstrate, in 2022, Verison found that data breaches, both accidental and deliberate, made up approximately 30% of cyber incidents within EMEA (Europe, the Middle East, and Africa) [2].

The Department for Culture, Media and Sport (DCMS) repeatedly found that charities are less cyber proficient than their private sector counterpart (this fact has been noted by DCMS across several Breach Survey Reports), citing a number of different reasons for this, ranging from a lack of awareness, to having an ad hoc approach to cyber security, based on informal advice, to charities believing they are not worth attackers' efforts [3].

Like many smaller organisations in the public sector, charities tend to focus on spending their income to deliver the services they were set up to provide. This is not surprising, as donors are likely more supportive if the funding they donate is spent on delivering services, rather than on the administration of the charitable organisation [4]. For larger charities, because these tend to be managed in a similar fashion to industry large private businesses, they are more likely to have teams of cyber experts as part of their staffing. However, for smaller charities, these are often unable to afford having this type of expertise on the payroll, thus exposing them to cyber threats, including relatively simple cyber-attacks [5]. As a result, while awareness of both ethical and legal responsibilities to data privacy is present, there is a lack of privacy and cyber security awareness on how to effectively defend the electronic data once collected. Many volunteers in charitable organisations are of an older generation [6], perhaps as they have more time to give in their retirement years, and the older generation is not as technically well versed as the younger generations. According to [7], it is the fear of vulnerabilities (viruses, phishing, fraud, etc.) and the using of technology that makes the older generation more adverse to adopting it.

Another aspect that charities must consider is the additional roles or types of data subject whose data they process, adding complexity to an already challenged sector. Whereas traditional businesses will typically deal with data from a few different data subject roles or types (e.g., staff, customers and suppliers), charities must also account for donors (who give funds), volunteers (unpaid workers) and beneficiaries (recipients of the service or benefit the charity provides), meaning they must also accounted for these roles, adding extra layers of consideration into their data-processing practices.

In addition, how data are handled by the charity can also be problematic; for example, once data have been centralised, e.g., by organising them and storing them in a database or in a customer relationship management (CRM) application, they can be described as structured data [8]) and should be relatively easy to manage. Data collected, created, or stored outside of this controlled format may be described as unstructured data [9], and handling this type of data can be daunting for organisations, as it ideally requires a managed approach in the form of taxonomy, indexing or classification [10].

Work to update frameworks to accommodate the protection of personal data has already started; for instance, ISO 27001, the ISO standard for information security management [11], has been enhanced with ISO 27701:2019, providing security techniques for privacy information management [12]. However, these frameworks are generic to organisations as opposed to catering specifically for a particular industry or sector.

A further problem is the volume of reading required for data privacy compliance, as has been reflected in DCMS in their 2018 Breach Survey Report, where one charity commented that “short and snappy” documentation would be more desirable for charities to review [13]. Smaller to medium size organisations (SMEs) may not have an obligation to appoint a Data Protection Officer (DPO), depending on the volume of records that are processed, and how sensitive the personal data being processed are [14]. Therefore, smaller charities and SME may not possess the necessarily skills and experience in-house to implement effective data privacy practices.

All organisations have a duty of care to safely handle our personal data and protect our right to a private life. While this right is assured through legislation in the United Kingdom (UK), we all have some aspects of our personal lives that we would rather keep more private than others, particularly when things are not going as well as we might like, and it is at times like these that we may seek or need the support of charitable organisations for help, and therefore, we argue that not-for-profit organisations and charities have a duty of care above and beyond their legal obligations when managing our personal data.

Thus, in this paper, we present a data privacy framework called “Privacy Essentials!”, designed to enable not-for-profit and charitable organisations to better understand their obligations, both from regulatory and legislative perspectives, as well as societal expectations when managing the privacy of stakeholders and digital information. We argue that a vibrant information security culture will benefit an organisation more than adding technical controls. To this end, it is vital for any organisation, including charities, to establish a solid foundation of procedures, processes and policies that complements the mission statement of the charity, thereby improving the organisation’s security posture. This is what this paper seeks to achieve through building a framework, Privacy Essentials!, applied specifically for the charity sector, providing them with a baseline of documentation that any charity can implement within their business. The idea is that Privacy Essentials! will benefit the charity by demystifying some of the perceived complexity when handling personal and/or sensitive data [15].

2. Background

As described in Section 1, within the charitable sector, when it comes to effectively managing data privacy, particularly for smaller charities, there are several problem domains that may arise, including the perception that achieving data protection is problematic [16]. This can be due to any number of the many factors that influence it as depicted in Figure 1. Within larger organisations, which have processes and skilled staff in place, they may well have a high security awareness, and thus, the issue is not considered problematic. However, for smaller charities, which may not be as robust in their security awareness, it has been suggested that the regulations may prove difficult to implement [17], and thus, we contend this framework's outcomes will benefit any charitable organisation in trying to overcome these perceived problems, while allowing the charity to realise further benefits by being responsible custodians of personal data.

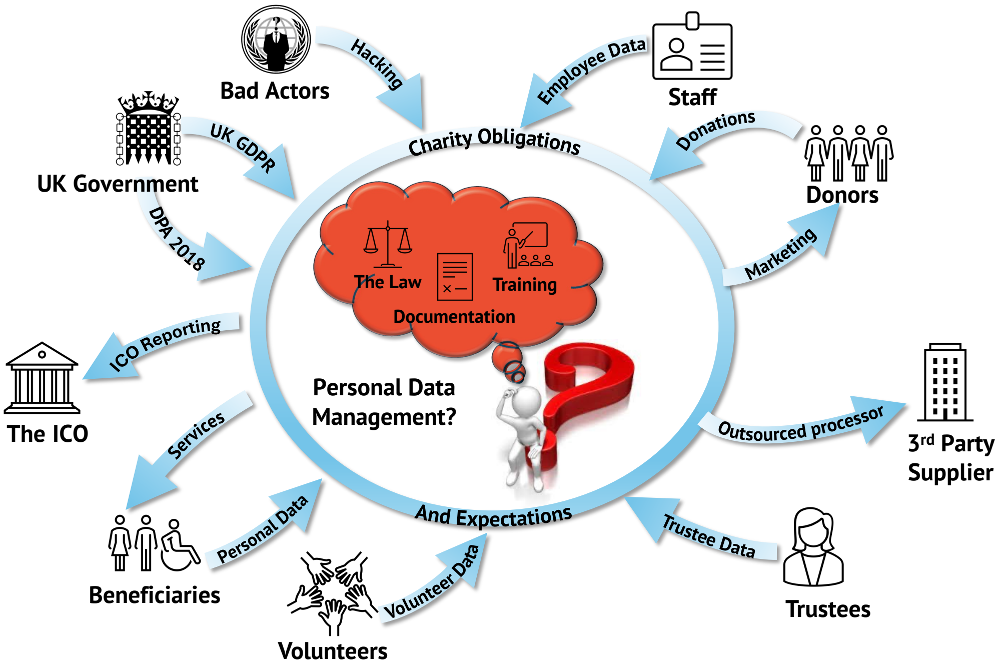


Figure 1. Data Privacy-Rich Picture

Uchendu et al. [18] noted that organisations can enhance a cyber security culture when management drives this and supports it with appropriate policy, procedures, and awareness. In addition, having a visible security culture will aid charities both in soliciting donors (customers) and in retaining them, which, over time will lead to increased brand trust and loyalty [19]. Moreover, charities that embrace the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) as having a positive impact on their operations will arguably reap these benefits, as well as managing personal data efficiently.

2.1. *The Right to Privacy*

Some industry sectors have historically had a robust position regarding confidentiality, for example, the banker considers customer privacy to be fundamental to the industry, born from the principles of morality and professionalism [20]. Likewise, a GP considers patient confidentiality to be an integral part of dealing with medical matters, a value that can be traced back to Hippocrates and remains a principle that is practised today [21].

In the UK, there was no specifically recognised legal right to privacy until the late 1990s, notably, the Protection from Harassment Act 1997, enacted to meet the obligations of the UK with regards to the European Convention of Human Rights, and, as regards digital data, the Data Protection Act 1998 [22]. Following on from these initial statutory provisions, in 2018, the General Data Protection Regulation (GDPR) came into effect across the European Union (EU) [8], and while the UK has now left the EU, the Data Protection Act 2018 (DPA 2018) has been enacted to incorporate the provisions of GDPR into UK law [23].

2.2. DPA 2018 and UK GDPR

There are other laws and regulations designed to protect UK subjects; however, for the purpose of this study, we elected to concentrate on DPA 2018, as this legislation has been devised to provide the privacy obligations for managing data that organisations must abide by. As part of this, Gov.uk sets out six data protection principles as outlined in [24] that align with GDPR Article 5(1). For the purposes of Privacy Essentials! we have also included, the seventh GDPR principle of accountability (GDPR Article 5(2)) for completeness (Table 1).

Table 1. Data protection principles.

Principle No	Principle	Meaning	GDPR Article
P1	Lawfulness, fairness and transparency	Data must be used fairly, lawfully and transparently; (DPA 2018, first principle, s. 35(1))	5(1)(a)
P2	Purpose limitation	Data are to be used for specified, explicit purposes; (DPA 2018, second principle, s. 36(1a))	5(1)(b)
P3	Data minimisation	Data are used in a way that is adequate, relevant and limited to only what is necessary; (DPA 2018, third principle, s. 37)	5(1)(c)
P4	Accuracy	Data must be accurate and, where necessary, kept up to date; (DPA 2018, fourth principle, s. 38(1a))	5(1)(d)
P5	Storage limitation	Data are kept for no longer than is necessary; (DPA 2018, fifth principle, s. 39(1))	5(1)(e)
P6	Integrity and confidentiality (security)	Data are handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage; (DPA 2018, sixth principle, s. 40)	5(1)(f)
P7	Accountability	Accountability requires organisations to take responsibility for how data are handled as well as compliance with the above principles. [25]	5(2)

The Information Commissioner's Office (ICO) also states that the categories of personal data outlined in Table 2 require stronger protection under UK GDPR Article 9.1.

Table 2. Special category data requiring stronger protection (UK GDPR Art. 9(1)).

Race
Political Opinions
Ethic background
Religious beliefs
Trade union membership
Genetics
Health
Sex life or orientation

Furthermore, personal data relating to criminal convictions and offences as outlined in UK GDPR Article 10 also require additional safeguards to be in place.

2.2.1. DPA Individual Rights and Processing of the Records

The UK GDPR also confers rights onto data subjects (the individual's whose data the organisation handles); these rights are outlined in Table 3.

Table 3. Individual rights.

Individual Right	**DPA 2018 or UK GDPR Reference**
Be informed about how your data are being used	DPA 2018, s. 44(1c))
Access personal data	DPA 2018, s. 45(1b)
Have incorrect data updated	DPA 2018, s. 46(1)
Have data erased	DPA 2018, s. 47(1)
Stop or restrict the processing of your data	DPA 2018, s. 49
Data portability	UK GDPR Article 20
Object to how your data are processed in certain circumstances	DPA 2018, s. 99(1)
There are additional rights when an organisation uses personal data for the following purposes:	
Make automated decision-making processes Profiling, for example, to predict your behaviour or interests	DPA 2018, s. 50 DPA 2018, s. 33(4)

When processing personal data, UK GDPR Article 30.1 requires that controllers maintain a record of how these personal records are processed by placing a requirement for the organisation to document as set out in Table 4.

Table 4. Records of processing activities (GDPR Art. 30(1)).

Article	DPA 2018 or UK GDPR Reference
30(1)(a)	The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer
30(1)(b)	The purposes of the processing
30(1)(c)	A description of the categories of data subjects and of the categories of personal data
(30(1)d)	The categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations
30(1)(e)	Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards
30(1)(f)	Where possible, the envisaged time limits for the erasure of the different categories of data
30(1)(g)	Where possible, a general description of the technical and organisational security measures referred to in Article 32(1) [or, as appropriate, the security measures referred to in Section 28(3) of the 2018 Act]

2.2.2. Data Protection Impact Assessment (DPIA)

As regards privacy risk, the ICO advises that a DPIA should be undertaken as part of an organisations' accountability obligations at the start of any new project, or when there are changes made to existing processes [26]. This requirement can be found within DPA 2018 chapter 4, Section 64 (1) and 64(4).

The definition for high risk has been adopted from the European Data Protection Board (EDPB), covering a wide range of processing operations [27] including the following:

- Large-scale profiling (although no specific number to define "large scale" is presented);
- The use of innovative technology (including artificial intelligence);
- Matching data obtained from multiple sources (e.g., in 2017, the ICO fined 11 charities GBP 138 k for profiling and matching potential donors [28]);
- Denial of service (based on automated profiling);
- Risk of physical harm;
- Collection of genetic or biometric data;
- Invisible processing (typically related to third party collection of data);
- Tracking an individual's behaviour or geolocation;
- Targeting vulnerable persons or children for marketing or automated decisions.

Further, the ICO cautions that while some might consider that the definition of "high risk and "large scale" is too vague [29], there is still no definitive template to follow in conducting a DPIA [26]. This is because while personal data types will share some common characteristics across the charity sector, e.g., name, e-mail, phone number, etc., how each organisation processes them will vary too widely for a framework to consider effectively. However, certain activities could arguably produce a partly filled template for a charity to complete, such as hiring employees, accepting donations, or delivering benefits.

Any breach, or suspected breach, of personal data, provided that the breach poses a risk to peoples' rights and freedoms, must be reported to the ICO within 72 h of the charity becoming aware that a breach has, or may have, occurred [30]. The ICO will then consider, based on how severe the breach is and what measures and technical controls are in place within the charity to protect personal data, what action to take. The ICO has the power to take action against the charity, including imposing significant fines dependent on the outcome of their investigation [31].

Where it is found that harm has potentially been done to an individual whose data were breached, the organisation may be liable to compensate the individual for that harm, which may prove costly, depending on the severity of the harm [32]. Recovery expenses, compensation, legal fees, reputational damage, regulatory fines, etc., are just some of the potential costs. However, it is worth bearing in mind that regarding how a charity reacts to a data breach, any loss of trust and/or reputational damage can be mitigated by being prepared. This means that having an effective incident response plan in place is important. Thus, a plan that incorporates sincere and apologetic strategies can help an organisation positively recover from a breach [33].

2.3. Data Protection by Design and Default

DPA 2018 Section 57 requires organisations to implement data protection by design and default (DPPbDD, s. 25), which requires that appropriate organisational and technical measures are implemented to both protect personal data (s. 57(1a)), and to ensure the data are being processed for the specific purpose they were received (s. 57(3)).

The intention is for the framework developed through this study to incorporate these principles, and those others discussed that are relevant (e.g., see Section 2.2), as an integral part of the development of the Privacy Essentials! framework.

2.4. Data Protection and Digital Information Bill

The Data Protection and Digital Information Bill is a new piece of legislation, currently being proposed by the UK government, devised to make changes to both UK GDPR and PECR [34]. The initial proposal did not pass the first reading in favour of an amended second bill for parliament to consider. Whilst this second bill was, at the time of undertaking this study, in the early stages of proposal, this literature review would be remiss to guess the impact of the final draft; however, it is important to note the law continuously changes and adds further complexity to personal data management to keep up to date with changes. At the time of writing, this bill has now reached the committee stage, so it looks likely that this might progress through to the final stages and enactment [34].

In addition to the aforementioned regulations, the Fundraising Regulator (FR) works within the confines of the law and, as part of their remit, provides standards to which charities are obliged to adhere [35]. Upon reviewing this, while we acknowledge this is an excellent resource and a code of conduct for charities, it does not provide anything to assist in developing policy or procedures for privacy.

2.5. Existing Frameworks

Several frameworks were identified that could provide guidance for best practice in managing privacy and cybersecurity. While some may consider these frameworks cumbersome, they do provide a useful reference point and checklist which can be used by charities to ensure their procedures or processes are appropriate and well founded, and therefore, these frameworks were reviewed as part of this study.

2.5.1. National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) was founded in 1901 NIST are part of the United States (US) Department of Commerce. One of the core competencies of NIST is the development and use of standards [36], including the NIST Privacy Framework that proposes five functions devised to complement the NIST Cybersecurity Framework as set out in Table 5 [37].

Table 5. NIST core privacy functions.

No	Function	Description
1	Identify	Develop the organisational understanding to manage privacy risk for individuals arising from data processing.
2	Govern	Develop and implement the organisational governance structure to enable an ongoing understanding of the organisation's risk management priorities that are informed by privacy risk.
3	Control	Develop and implement appropriate activities to enable organisations or individuals to manage data with sufficient granularity to manage privacy risks.
4	Communicate	Develop and implement appropriate activities to enable organisations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.
5	Protect	Develop and implement appropriate data processing safeguards.

In the US, privacy laws differ between the states, and only a few laws are universal across the country, and those privacy regulations have tended to be focused on particular industries, such as the Health Insurance Portability and Accountability Act (HIPPA), as opposed to Europe, where privacy is treated and dealt with through the one regulation, GDPR, regardless of the industry sector [38]. As a result, the NIST privacy framework has been devised to address a large variety of use cases, rather than any unified set of laws, which is one of the advantages of NIST, as it provides appropriate guidance that can be easily adapted for our purposes.

2.5.2. International Organisation for Standardisation (ISO)

The International Organisation for Standardisation (ISO) provides 'global standards' for all manner of subjects that are agreed upon internationally by experts in each field [39], including privacy and security. For privacy, ISO/IEC 27701:2019 provides a privacy extension to ISO/IEC 27001, the ISO security management standard developed for the international community. ISO 27701 incorporates many of the security controls from the main standard into the privacy framework to help organisations improve their privacy information management [12].

ISO 27701 formalises the process of a Privacy Information Management System (PIMS), as well as assisting with the auditing of the processes and management reviews [40]. As part of this standard, ISO recommends controls to protect and manage personal data. The regulations themselves (GDPR, and DPA) do not specify controls deliberately, rather, they leave the details of how to protect personal data for the organisation to define themselves [41].

2.5.3. Cyber Essentials

The National Cyber Security Centre (NCSC) introduced Cyber Essentials, a UK government scheme devised to assist organisations in defending themselves from common cyber-attacks [42]. There are two Cyber Essentials programmes as part of this scheme, Cyber Essential and Cyber Essentials Plus, both of which reference technical controls to maintain a secure network [43]. The intention for this study is to use this framework to support and cross-reference to support the process documentation.

2.6. Data Taxonomy, Classification, and Access Control Frameworks

In managing data, it is useful to classify the data so that only authorised staff and or approved applications can view or access, based on appropriate user permissions, thereby allowing the organisation to adopt either Role-Based Access Controls (RBAC), i.e., access based on user role within the business, or Mandatory Access Controls (MAC), i.e., access based on the policy for objects [44]. These access control frameworks help in understanding, planning and managing user roles for both structured and unstructured data.

However, it is important to keep data classification relatively simple and the naming conventions obvious, to make it easier for the user. For instance, Public > Personal > Personal Sensitive > Confidential will likely meet most needs, especially if the UK government only uses three levels [45].

The disadvantage of classifying data is in ensuring that users classify documents in accordance with the agreed conventions. In the case of charity organisations, using pre-classified templates and ensuring that proper training is delivered to new employees or volunteers upon joining the charity will help ensure they fully understand how to classify documentation correctly [46]. Metadata can also assist with data classification, and using authors name, tags, last saved date, etc., can all potentially assist in searching for documentation, as well as in reviewing for data retention considerations.

3. Methodology

This research aimed to improve privacy management in charities through collaboration, using Action Research for its participatory approach [47]. All the ethics approvals were granted by the University Ethics Committee. The primary collaborator was a Dorset-based cancer charity, with stakeholders including key staff, senior management, operations, volunteers, finance, and marketing. Two other charities were consulted for broader applicability.

The study had three iterations:

- Data collection (Section 4), which involves secondary data (Sections 2, 2.5, 4.1 and 4.2) and primary data from client interviews (Section 4.3) to develop personas, user stories, document analysis, and Volere requirements (Sections 4.4–4.7).
- Design (Section 5), which includes creating the framework in Ms Excel v.16.85. In order to achieve that, we collected the requirements by meticulously analysing the existing privacy policy and regulations, applying requirement analysis with the results of the client interviews against the scope of the framework and implementing the framework with workflow diagrams and data flow diagrams.
- Evaluation (Section 6), where the framework was assessed by the client and collaborators using the System Usability Score (SUS) survey and Morville's UX honeycomb [48,49].

4. Data Collection

4.1. Analysis of UK GDPR

All organisations that collect and process personal data must comply with the UK GDPR and, as part of this, document how such data are processed within the organisation (Table 6) [50], and keep accurate records of certain activities.

Table 6 lists all documentation requirements charities must conform with in order to be fully GDPR compliant. Note, however, that further documentation requirements will apply, where a charity transfers data outside of the European Economic Area (EEA) as part of their processing (Table 4, or if they require a DPO).

Table 6. Mandatory UK GDPR documentation.

Documentation	Article
Privacy Notice	Articles 12, 13 and 14
Employee Privacy Notice	Articles 12, 13 and 14
Personal Data Protection Policy	Article 24
Data Retention Policy	Articles 5, 13, 17 and 30
Data Retention Schedule	Article 30
Data Subject Consent Form	Articles 6, 7 and 9
Parental Consent Form	Article 8
DPIA Register	Article 35
Supplier Data Processing Agreement	Articles 28, 32 and 82
Data Breach Response and Notification Procedure	Articles 4, 33 and 34
Data Breach Register	Article 33
Data Breach Notification Form to the Supervisory Authority	Article 33
Data Breach Notification Form to the Data Subjects	Article 34

4.2. Analysis of Existing Frameworks

ISO and NIST are excellent resources for helping organisations define personal data management practices as part of their privacy by design and by default (DPPbDD) recommendations (Section 2.3). Table 7 compares ISO guidance to the relevant GDPR principles [12]

Table 7. Comparison of GDPR principles and ISO recommendations.

GDPR Principle	ISO Recommendation
Principle (b): Purpose limitation	7.4.2 Limit processing: The organisation should limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes.
Principle (b): Purpose limitation	7.4.6 Temporary files: The organisation should ensure that temporary files created as a result of the processing of PII are disposed of (e.g., erased or destroyed) following documented procedures within a specified, documented period.
Principle (c): Data minimisation	7.4.1 Limit collection: The organisation should limit the collection of PII to the minimum that is relevant, proportional, and necessary for the identified purposes.
Principle (d): Accuracy	7.4.3 Accuracy and quality: The organisation should ensure and document that PII is as accurate, complete and up to date as is necessary for the purposes for which it is processed, throughout the life-cycle of the PII.
Principle (e): Storage Limitation	7.4.7 Retention: The organisation should not retain PII for longer than is necessary for the purposes for which the PII is processed.
Principle (f): Integrity and confidentiality	7.4.9 PII transmission controls: The organisation should subject PII transmitted (e.g., sent to another organisation) over a data transmission network to appropriate controls designed to ensure that the data reach their intended destination.

Privacy Essentials! incorporated these principles within the Policy and Procedure documentation as well as within the technical controls appropriate for the protection of personal data that is processed electronically, including access control lists, encryption, password control, and protective marking and awareness training.

Next, common technical control measures from ISO [12] and NIST Data Protection Clauses [37], such as encryption, access control lists, protective marking, passwords, and awareness training, were analysed and those deemed relevant were incorporated.

4.3. Client Interviews

In total, four interviews were conducted with the client, each scheduled for an hour. The first interview was conducted with the client's CEO to present a brief overview of the project and the expected involvement. As part of this meeting, desired outcomes for the charity and how the framework might assist them going forward were discussed. The client considered that the proposed framework would prove very helpful to the sector.

Two further interviews were conducted with senior members of staff, both seasoned workers within the charity sector, who were responsible for controlling data collection and the processes of data within the charity. This allowed insight that not only reflects the needs of the client charity but also provides a wider context within the sector for the study to consider.

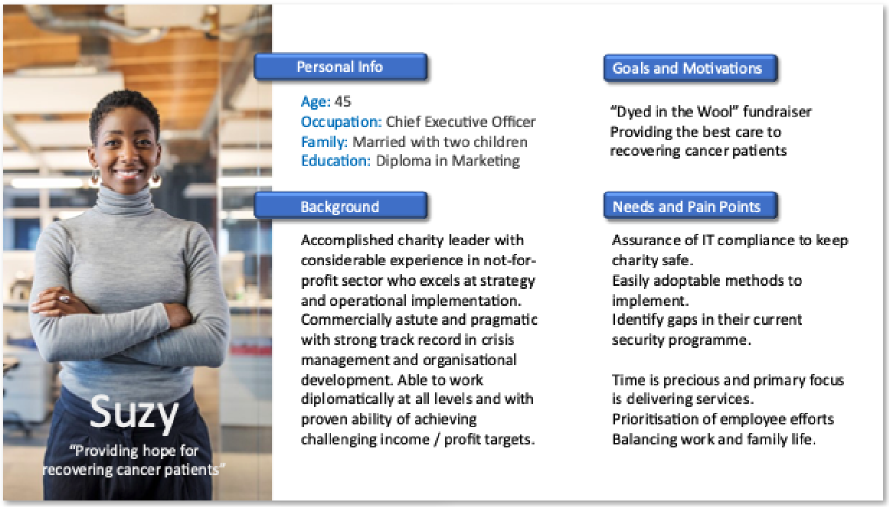
Next, an interview with a trustee for the client was carried out. This trustee is a director of a managed service provider, and, as such, able to provide useful observations regarding the inclusion of processes within the framework. This stakeholder considered that the study should be documentation focused rather than interpretation focused, thus leaving the technical interpretation to individual IT teams.

4.3.1. Expert Advisor Interview

A final interview was conducted with a privacy data matter expert, certified as an EU General Data Protection Regulation Practitioner (IBITGQ), who is also a board member of a charity. This interview was conducted to verify the feasibility of the study and its outcomes. This interview was scheduled for 45 min to discuss the functionality and outcomes of the framework. Keeping the framework simple to use while allow sufficient transferring of knowledge about data privacy obligations were useful discussion points. In addition, discussion was held around what policies and procedures would need to be included in the documentation pack to make the framework as relevant as possible.

4.4. Personas

The implementation of a privacy or security framework is a management consideration [51]; whilst improvements to the framework can be driven from external sources or any member(s) of staff, the initiation of implementation has to come from the board. To support the requirements and help facilitate easy-to-understand comprehension of the requirements gathered from the interviews for the client to review and agree, three charity board personas were created as depicted in Figures 2–4.



Suzy

"Providing hope for recovering cancer patients"

Personal Info

Age: 45
Occupation: Chief Executive Officer
Family: Married with two children
Education: Diploma in Marketing

Background

Accomplished charity leader with considerable experience in not-for-profit sector who excels at strategy and operational implementation. Commercially astute and pragmatic with strong track record in crisis management and organisational development. Able to work diplomatically at all levels and with proven ability of achieving challenging income / profit targets.

Goals and Motivations

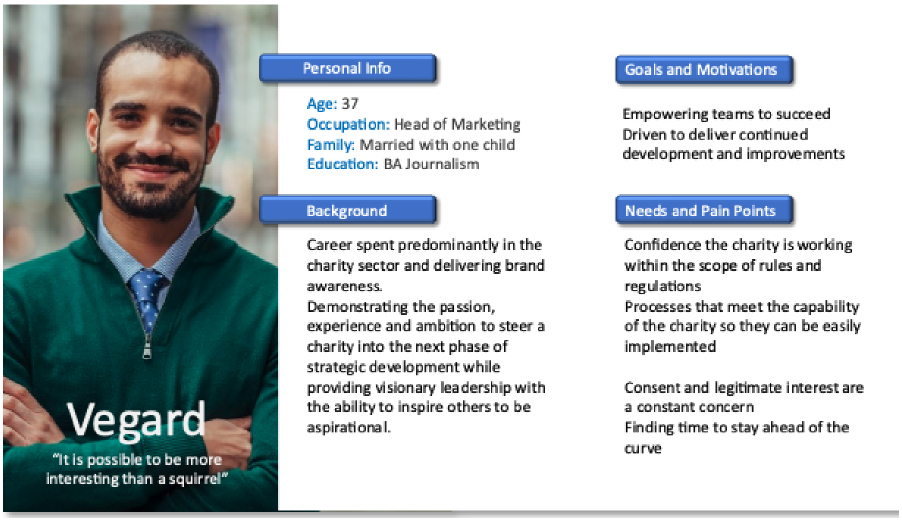
"Dyed in the Wool" fundraiser
Providing the best care to recovering cancer patients

Needs and Pain Points

Assurance of IT compliance to keep charity safe.
Easily adoptable methods to implement.
Identify gaps in their current security programme.

Time is precious and primary focus is delivering services.
Prioritisation of employee efforts
Balancing work and family life.

Figure 2. Persona, Chief Executive Officer



Vegard

"It is possible to be more interesting than a squirrel"

Personal Info

Age: 37
Occupation: Head of Marketing
Family: Married with one child
Education: BA Journalism

Background

Career spent predominantly in the charity sector and delivering brand awareness.
Demonstrating the passion, experience and ambition to steer a charity into the next phase of strategic development while providing visionary leadership with the ability to inspire others to be aspirational.

Goals and Motivations

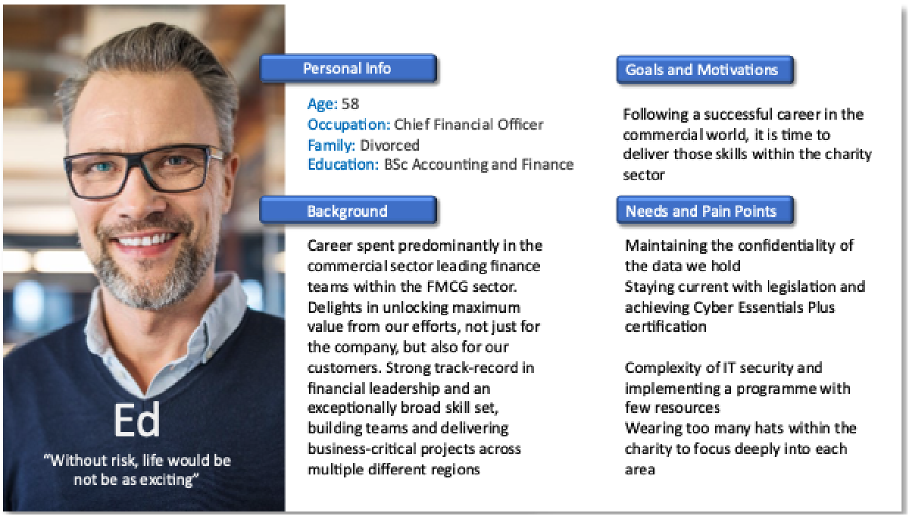
Empowering teams to succeed
Driven to deliver continued development and improvements

Needs and Pain Points

Confidence the charity is working within the scope of rules and regulations
Processes that meet the capability of the charity so they can be easily implemented

Consent and legitimate interest are a constant concern
Finding time to stay ahead of the curve

Figure 3. Persona, Head of Marketing



Ed

"Without risk, life would be not be as exciting"

Personal Info

Age: 58
Occupation: Chief Financial Officer
Family: Divorced
Education: BSc Accounting and Finance

Background

Career spent predominantly in the commercial sector leading finance teams within the FMCG sector.
Delights in unlocking maximum value from our efforts, not just for the company, but also for our customers. Strong track-record in financial leadership and an exceptionally broad skill set, building teams and delivering business-critical projects across multiple different regions

Goals and Motivations

Following a successful career in the commercial world, it is time to deliver those skills within the charity sector

Needs and Pain Points

Maintaining the confidentiality of the data we hold
Staying current with legislation and achieving Cyber Essentials Plus certification

Complexity of IT security and implementing a programme with few resources
Wearing too many hats within the charity to focus deeply into each area

Figure 4. Persona, Head of Finance

4.5. User Stories

MoSCoW (Must have, Should have, Could have, Won't have) is a useful framework to prioritise requirements as part of progressing a study against a timeline [52], meeting deadline restrictions and recognising improvements to incorporate in future iterations. Thus, from the interviews, several user stories were created to first depict requirements in an easily followed format for non-technical stakeholders [53] (the interviewees) and to help build out the requirements for Privacy Essentials! framework. These user stories are shown in Table 8.

Table 8. User stories—MoSCoW requirements.

ID	Must Have	Considerations	Origin
M.1	As the CEO, I must be able to establish data privacy policy and procedures that outlines how our data are managed in compliance to the law	Privacy Essentials! will reference the applicable laws and regulations where possible.	Interview
M.2	As the Marketing Director the framework must identify any gaps in our compliance to that we can rectify	The Framework will keep to plain English and try to avoid technical jargon or acronyms	Interview
M.3	As the Finance Director the framework must be presented in easy-to-understand terms.	Privacy Essentials! will reference the applicable laws and regulations where possible.	Interview
	Should Have		
M.4	As the Marketing Director, the framework should have policies that I can adapt to assure potential donors their privacy is assured	This will be covered in the Privacy and Procedures pages	Interview
M.5	As the privacy expert, the framework should build a risk register for the personal data collected	Article 30 considerations are part of the framework, it will not be as thorough as the ICO-but overtime will be	Interview
M.6	As the Finance Director, the framework should recommend if a DPO is required	This can be added to the recommendations page if special category data are present	Interview
M.7	As the CEO the framework should be specific to the charity sector to capture our requirements	Most personas are catered for within the framework	Interview
	Could Have		
M.8	As the Researcher this framework could have been written in HTML to enable a web-based application	It could have, however with a working copy in Excel, it may be possible to convert to HTML	Interview
M.9	As the privacy expert the framework could create data processing impact assessments	DPIA template will be provided and instructions on use, however difficult to auto-fill	Interview
M.10	As the Finance Director the framework could have PCI DSS considerations to aid in achieving compliance to the standard	PCI DSS is a different discipline, although many of the considerations to achieve UK GDPR compliance are similar. Not included in this iteration	Interview
	Won't Have		
M.11	As the researcher for the framework, the tool won't have Macros enabled to allow risk free evaluations	The researcher would like them as it helps when testing, however other automation techniques are used	Interview
M.12	As the Trustee, the framework won't have processes as this is too cumbersome to implement on our own	Processes were part of the original plan, however, in agreement with the Trustee and will drop from project	Interview

4.6. Document Analysis

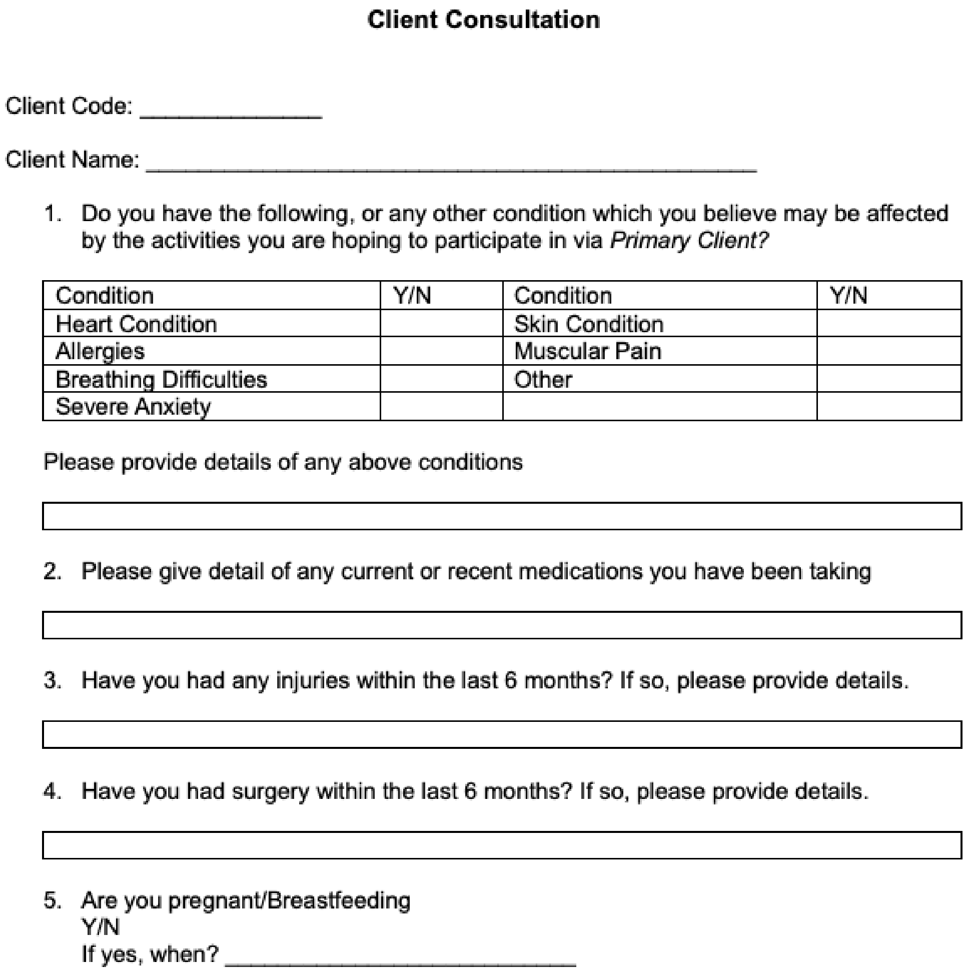
4.6.1. Data Capture Forms

As part of the interviews, discussion took place around what data are collected and the various forms and templates used to support the collection of that data. It transpired that some data are captured electronically at the point of contact, such as Gift Aid information within the charity's various high street stores, while other data are captured manually on templates, such as the one depicted in Figure 5.

A further six templates used for data collection were provided by the client for analysis:

- New volunteer request form;
- New staff starter form;
- Change request form;
- Request for IT services form;
- Marketing consent form;

- Client on-boarding check list (although this contained no personal data, falling outside of the scope of the project).



Client Consultation

Client Code: ______________

Client Name: ____

1. Do you have the following, or any other condition which you believe may be affected by the activities you are hoping to participate in via *Primary Client?*

Condition	Y/N	Condition	Y/N
Heart Condition		Skin Condition	
Allergies		Muscular Pain	
Breathing Difficulties		Other	
Severe Anxiety			

Please provide details of any above conditions

2. Please give detail of any current or recent medications you have been taking

3. Have you had any injuries within the last 6 months? If so, please provide details.

4. Have you had surgery within the last 6 months? If so, please provide details.

5. Are you pregnant/Breastfeeding
Y/N
If yes, when? ___________________________

Figure 5. Client consultation form (redacted).

From these forms, it was possible for us to compare and catalogue these form's fields and consider how the data could best be classified, using the recommended classifications of "Unique", "Personal", or "Sensitive". "Sensitive" was chosen, as this was considered more universally understood than the "Special Category" (as used with UK GDPR Article 9.1 (see Table 2). As seen in Figure 5, while the name of a client of the charity is captured, this may not be enough to render the remaining (sensitive data) personal. This is because on its own, a name will not necessarily uniquely identify a person. However, should access to the client code database be compromised, then the data captured would be linkable to an individual. An example of the data analysis for client consultation form provided is shown in Table 9.

Other data capture points captured from the interviews do exist (e.g., donors details, new employee starters, and trustees); however, those templates were not provided, although sufficient details about these were captured from the interview sessions to create similar analysis tables (see Appendix A).

Table 9. Analysis of client consultation forms.

Client Consultation Form	Personal	Sensitive	Unique	Comments
Client Code	No	No	No	Ideal for pseudonymisation
Client Name	Yes	No	No	When coupled with other data, could identify the person
Health Conditions, including allergies, heart or breathing condition, severe anxiety, skin condition, muscular pain or other	Yes	Yes	No	Special Category data
Current Medication	Yes	Yes	No	Special Category data
Injury details	Yes	Yes	No	Special Category data
Surgery details	Yes	Yes	No	Special Category data
Pregnancy Status	Yes	Yes	No	Special Category data
Breast Feeding	Yes	Yes *	No	* Personal-sensitive
Chemo or Radiation treatment	Yes	Yes	Yes	Sensitive as potential for fraud
Signature	Yes	Yes	No	Special Category data

Based on how sensitive data fields captured are, a Data Protection Officer (DPO) may be required to be appointed, and special attention paid to how data collected or received are managed, to ensure compliance with DPA 2018 (Section 2.2).

4.6.2. Workflow Analysis

Understanding how the charity processes data helped us in designing the framework. What it also did was to allow us to identify similarities between data management elements that could be considered common across the charity sector, thus allowing us to class these as common requirements. To facilitate this piece of work, we discussed workflows with the client, covering their processes, as well as the software applications being used to manage the business. In addition, work processes for fundraising, volunteer data, and client data, as well as gift aid were also shared by the client.

As part of the discussion from the interviews (Section 4), and the workflow analysis in this section, it also transpired that while some processing is managed in-house, others are outsourced, and that processing activity will also need to be captured by the framework to ensure it is accurately recorded, and that data are correctly managed and appropriate privacy treatment applied in those processes as well. Thus, the framework will need to incorporate a data risk register, and identify any third-party processors that are processing the charity's data. From this, we identified a number of processes that personal data are subjected to within the charity; these are listed in Table 10.

Table 10. Personal data processing.

Personal Data	Processed	Recommendation
Employee Recruitment	In-House	Ensure appropriate access controls and data protection measures
Employee Records	In-House	Ensure appropriate access controls and data protection measures
Payroll	Out-sourced	Confirm 3rd Party contracts are in place and Data held within the EAA (Section 2.2)
Donor Data	Salesforce (SaaS)	Confirm 3rd Party contracts are in place and Data held within the EAA (Section 2.2)
Donor Gift Aid	Azurri (outsourced)	Confirm 3rd Party contracts are in place and Data held within the EAA (Section 2.2)
Beneficiary Data	Airtable (outsourced)	Confirm 3rd Party contracts are in place and Data held within the EAA (Section 2.2)

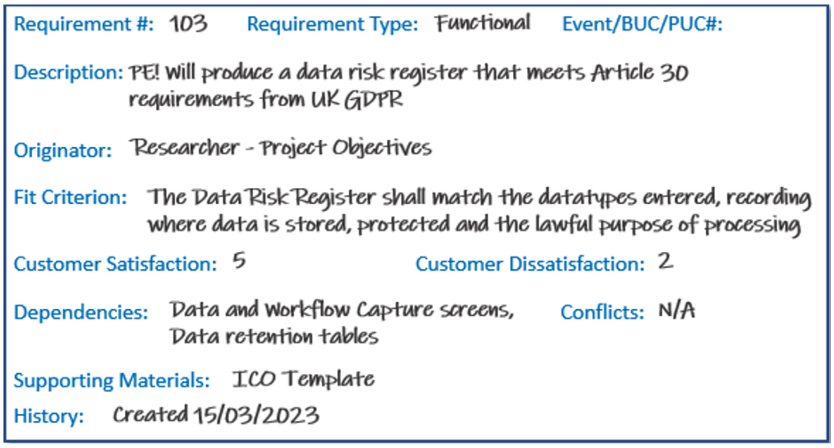
Table 10. *Cont.*

Personal Data	Processed	Recommendation
Trustee Data	Salesforce (SaaS)	Confirm 3rd Party contracts are in place and Data held within the EAA (Section 2.2)
Volunteer Data	Salesforce (SaaS)	Confirm 3rd Party contracts are in place and Data held within the EAA (Section 2.2)
Practitioner Data	Airtable (outsourced)	Confirm 3rd Party contracts are in place and Data held within the EAA (Section 2.2)

Understanding these requirements, consideration was given to the design of the framework, and how best to capture the relevant details as they pertain to the charity sector, and ensure relevant outcomes will be produced that are beneficial when seeking UK GDPR compliance.

4.7. Privacy Essentials! Volere Requirements

A complementary method for documenting requirements is to use the Volere Requirements Specification Template [54], producing "snow cards" to depict each requirement, and the attributes that contribute to that requirement. An example is show in Figure 6.



Requirement #: 103 Requirement Type: Functional Event/BUC/PUC#:

Description: PE! will produce a data risk register that meets Article 30 requirements from UK GDPR

Originator: Researcher - Project Objectives

Fit Criterion: The Data Risk Register shall match the datatypes entered, recording where data is stored, protected and the lawful purpose of processing

Customer Satisfaction: 5 Customer Dissatisfaction: 2

Dependencies: Data and Workflow Capture screens, Data retention tables Conflicts: N/A

Supporting Materials: ICO Template

History: Created 15/03/2023

Figure 6. Volere "snow card" requirement.

Thus, using Volere, all these individual requirements were summarised into a list of requirements for Privacy Essentials! (PE!), designed to complement the user story requirements outlined in Section 4.5, Table 8; this can be found in Table 11.

Table 11. Volere requirements table.

ID	Functional Requirements	Motivation	Origin
V.1	PE! shall provide all relevant policies for charities to consider	Draw attention to the mandatory documentation required as part of an ISMS.	Background Review (ICO, Section 4.2)
V.2	PE! shall automate Article 30 reporting	Simplify the task to build a template that is easily added to	Background Review (ICO, Section 4.2)
V.3	PE! shall identify sensitive data	Highlight the charities additional responsibilities when handling special category data	Background Review (NIST, Section 4.2)

Table 11. *Cont.*

ID	Functional Requirements	Motivation	Origin
V.4	PE! should recommend relevant procedures for charities to implement	Provide easy-to-understand procedures that are achievable	Background Review (DCMS, Section 1)
V.5	PE! should provide an action plan for the charity to progress	Break each task into its component parts that can be progressed	Expert Advisor (Section 4.3.1)
ID	**Non-Functional Requirements**	**Motivation**	**Origin**
	Look and Feel Requirements		
V.6	PE! shall be consistent in its design and functionality	Good design inspires confidence	Researcher commercial experience
V.7	PE! shall appear professional in style	Establish trust in the framework	Past Research-Human Factors
	Usability and Humanity Requirements [55]		
V.8	PE! should be intuitive to use	Establish trust in the framework	[55]
V.9	PE! should score above 68% with a first-time user in the charity sector	Establish trust in the framework	[48]
V.10	PE! shall highlight errors or cautions	Guide the user to make the framework helpful	[55]
V.11	The user must be familiar with data processing within the Charity	To maximise the potential gain from the framework	Interviews
V.12	PE! shall be written in English, language support for EMEA can be added later	Time to programme—later iterations can cater for multiple language support	[56]
V.13	PE! shall use universally recognised symbols to navigate the framework	Assists with intuitive use	[57]
	Performance Requirements		
V.14	PE! shall respond promptly to user input	Unnecessary delays can lead to frustration	Researcher experience
V.15	PE! shall reflect the current legislation and update as required	For the framework to be credible, it must be current	Background Review (Section 4.2)
	Operational and Environmental Requirements		
V.16	PE! shall work on a windows 11 OS running MS Excel	Provides a known platform for the coding to operate (iOS Excel does not work)	Researcher experience
	Maintainability and Support Requirements		
V.17	PE! shall be updated periodically as new features are requested and implemented	Ensure the product is current and free from any bugs or unexpected outcomes	Researcher commercial experience
	Security Requirements		
V.18	PE! shall be macro free and will be password protected	Encourages use without Microsoft warnings	Interviews
	Cultural Requirements		
V.19	None identified—PE! Implements UK GDPR	Potential to produce in Welsh	
	Legal Requirements		
V.20	PE! is the intellectual property of Cedars (2019) Ltd.	This framework, once validated, has commercial value	Cedars (2019) Ltd.

The researchers acknowledge that this document uses material from the Volere Requirements Specification Template, copyright © 1995–2020 the Atlantic Systems Guild Limited.

With the requirements defined from both MoSCoW (Table 8) and Volere requirements (Table 11), the next phase of designing the artefact can begin.

5. Design

The Privacy Essentials! framework was built within Microsoft Excel, a widely used application, accessible also through other spreadsheet applications, such as Google Sheets, LibreOffice spreadsheets or Apple Numbers. Further, the functions used as part of the design work equally well within the desktop and cloud versions of Excel.

5.1. Early Considerations

Upon starting the design process, it soon became clear there were two distinct considerations that needed to be considered: (a) the source of the data; and (b) the manner in which the data are processed. To obtain an overview of the data sources, a mind map was created (Figure 7), depicting each of the charity sector's seven distinct identities identified (legacy data were incorporated into donor data).

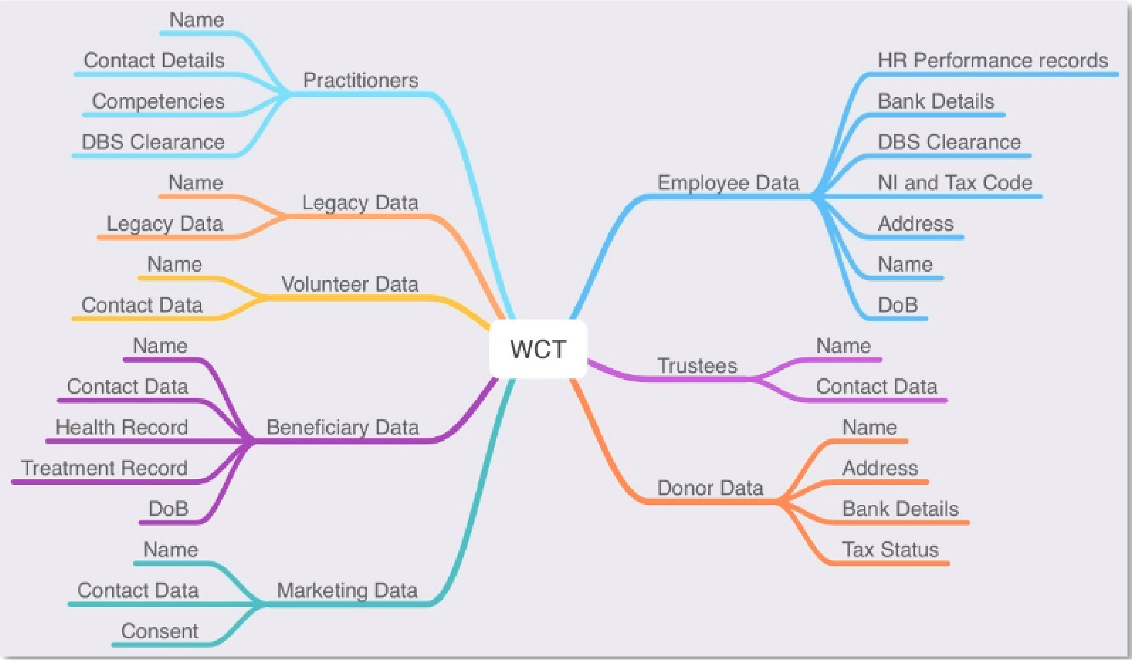


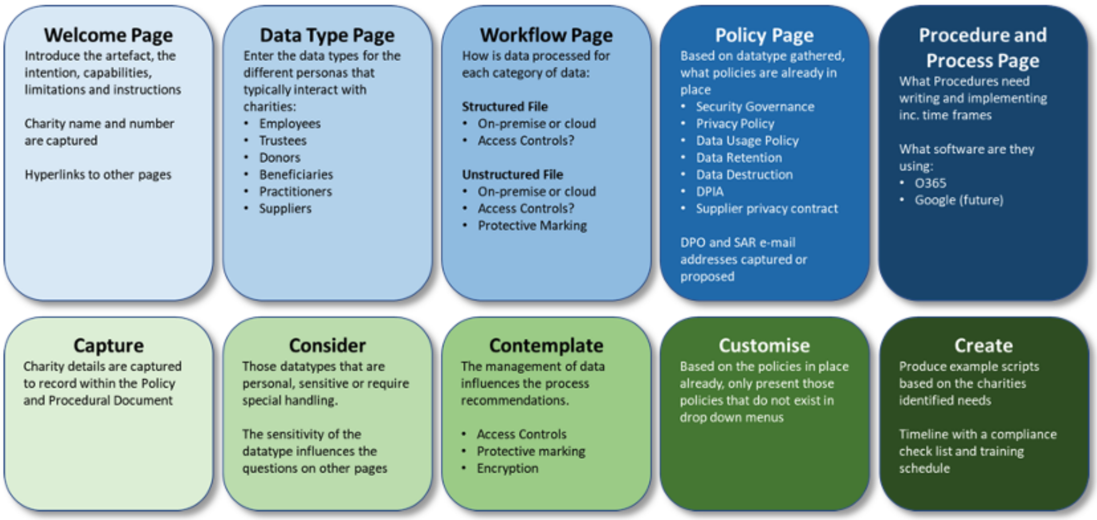
Figure 7. Mind map of entities and data types.

As outlined in Table 10, each identity has its own unique processing requirements, and thus, workflow pages could be designed to follow a similar categorisation. Following this rationale also aligns with the framework being able to produce Article 30 compliant documentation as required under the UK GDPR (Section 2.2, Table 6) and identified in requirements V.2 and M.5, Tables 8 and 11. This will allow the Privacy Essentials! (PE) framework to show the different purposes each data field is collected for and that data are processed lawfully, stored, and retained within a data risk register.

As part of this feature, PE collates some fields and auto categorises these as "personal details", such as as name, address, e-mail address, and phone numbers, to avoid the data collection form within the framework from requiring users to input too many repetitive responses.

5.2. Privacy Essentials! Work and Data Flow

Next, a diagram was created to outline the conceptual design, showing how data and workflow pages are separated within PE (Figure 8). This allows each page to remain compact and therefore not overwhelm the user with too much information.



Welcome Page
Introduce the artefact, the intention, capabilities, limitations and instructions

Charity name and number are captured

Hyperlinks to other pages

Data Type Page
Enter the data types for the different personas that typically interact with charities:
- Employees
- Trustees
- Donors
- Beneficiaries
- Practitioners
- Suppliers

Workflow Page
How is data processed for each category of data:

Structured File
- On-premise or cloud
- Access Controls?

Unstructured File
- On-premise or cloud
- Access Controls?
- Protective Marking

Policy Page
Based on datatype gathered, what policies are already in place
- Security Governance
- Privacy Policy
- Data Usage Policy
- Data Retention
- Data Destruction
- DPIA
- Supplier privacy contract

DPO and SAR e-mail addresses captured or proposed

Procedure and Process Page
What Procedures need writing and implementing inc. time frames

What software are they using:
- O365
- Google (future)

Capture
Charity details are captured to record within the Policy and Procedural Document

Consider
Those datatypes that are personal, sensitive or require special handling.

The sensitivity of the datatype influences the questions on other pages

Contemplate
The management of data influences the process recommendations.

- Access Controls
- Protective marking
- Encryption

Customise
Based on the policies in place already, only present those policies that do not exist in drop down menus

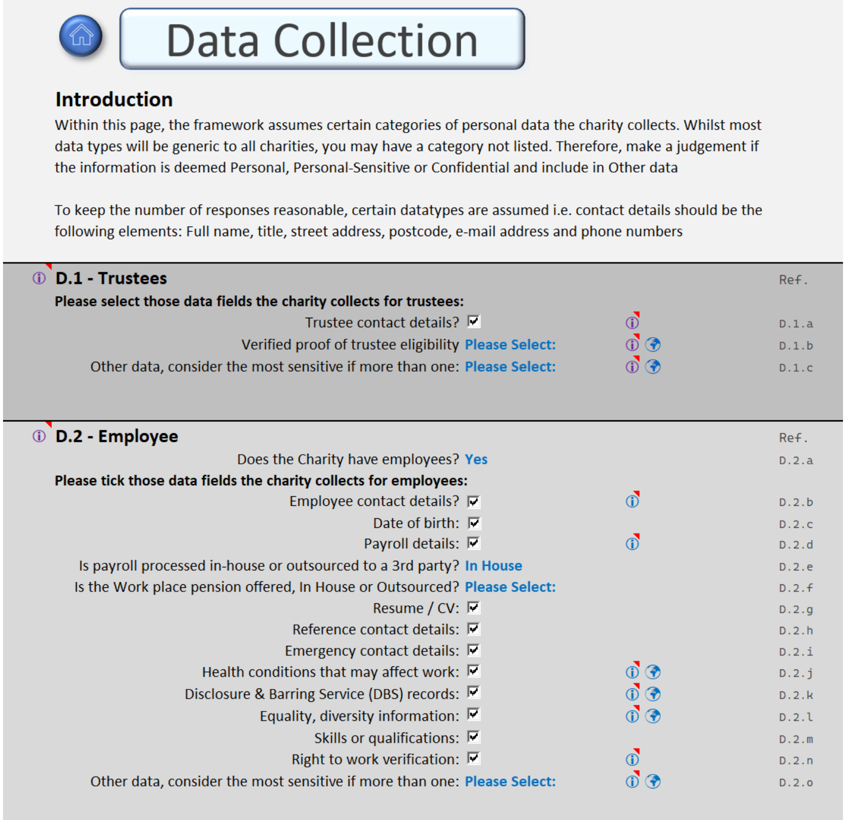
Create
Produce example scripts based on the charities identified needs

Timeline with a compliance check list and training schedule

Figure 8. Privacy Essentials! conceptual design.

5.3. Layout

Within Excel, there are some useful elements that are pre-built that facilitate the user to use form controls and drop-down menus to guide them through the form with pre-set acceptable answers to select from. This, in turn, allowed us to design the back-end processing so that this would process answers selected with definitive responses. As regards the questions, style questions were kept simple, and the client was consulted on certain preferences based on the options provided. For the layout, the client was consulted before the programming of PE commenced. An example of the data collection form sent to the client for evaluation can be found in Figure 9.



Data Collection

Introduction

Within this page, the framework assumes certain categories of personal data the charity collects. Whilst most data types will be generic to all charities, you may have a category not listed. Therefore, make a judgement if the information is deemed Personal, Personal-Sensitive or Confidential and include in Other data

To keep the number of responses reasonable, certain datatypes are assumed i.e. contact details should be the following elements: Full name, title, street address, postcode, e-mail address and phone numbers

ⓘ **D.1 - Trustees**			Ref.
Please select those data fields the charity collects for trustees:			
Trustee contact details?	☑	ⓘ	D.1.a
Verified proof of trustee eligibility	Please Select:	ⓘ 🌐	D.1.b
Other data, consider the most sensitive if more than one:	Please Select:	ⓘ 🌐	D.1.c
ⓘ **D.2 - Employee**			Ref.
Does the Charity have employees?	Yes		D.2.a
Please tick those data fields the charity collects for employees:			
Employee contact details?	☑	ⓘ	D.2.b
Date of birth:	☑		D.2.c
Payroll details:	☑	ⓘ	D.2.d
Is payroll processed in-house or outsourced to a 3rd party?	In House		D.2.e
Is the Work place pension offered, In House or Outsourced?	Please Select:		D.2.f
Resume / CV:	☑		D.2.g
Reference contact details:	☑		D.2.h
Emergency contact details:	☑		D.2.i
Health conditions that may affect work:	☑	ⓘ 🌐	D.2.j
Disclosure & Barring Service (DBS) records:	☑	ⓘ 🌐	D.2.k
Equality, diversity information:	☑	ⓘ 🌐	D.2.l
Skills or qualifications:	☑		D.2.m
Right to work verification:	☑	ⓘ	D.2.n
Other data, consider the most sensitive if more than one:	Please Select:	ⓘ 🌐	D.2.o

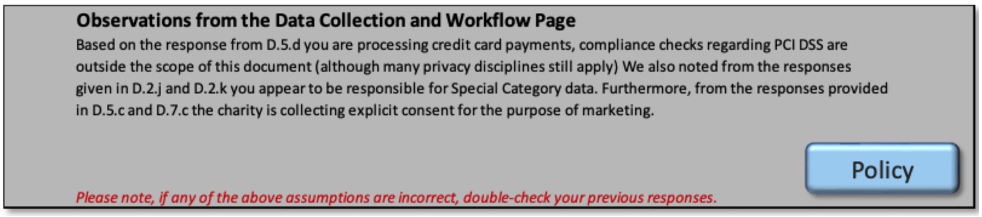
Figure 9. Privacy Essentials! data collection form.

Feedback on the layout feedback was received via email from the client with all three charity interviewees participating (Section 4.3). Their feedback and observations helped define the style for PE. As part of this, icon preferences (as per requirement V.13 in Table 11) were confirmed: 🌍 is used for web-links, whilst ℹ is used for additional information instead of a "**?**". Similarly, changing the way questions were displayed, from horizontal to vertical, was requested by the client.

In addition, the clients suggested that a more colourful palette would improve PE. However, because the lead developer on PE is colour-blind, and to accommodate other users who may also be colour-blind, a monochrome schema was selected and used [58]. Settings for preferences for fields with tick boxes or drop-down menus were also discussed, with a defaulted "No" preset for tick-boxes and a "Please select" pre-set for drop-down menus, as these require an active response.

5.4. Programming Privacy Essentials!

PE is programmed to be dynamic and reliant on previous responses before presenting or generating the next sections or tabs. To facilitate this, error, cautionary, or advisory messages reflect on past answers given by the user to deliver their message. This is performed to allow PE to provide a check-back message before moving the user on to the next stage(s), or to affirm the entries made. For example, as shown in Figures 10–13, we can see how the Workflow tab builds out into a series of three statements that references previous questions generated from the observations.

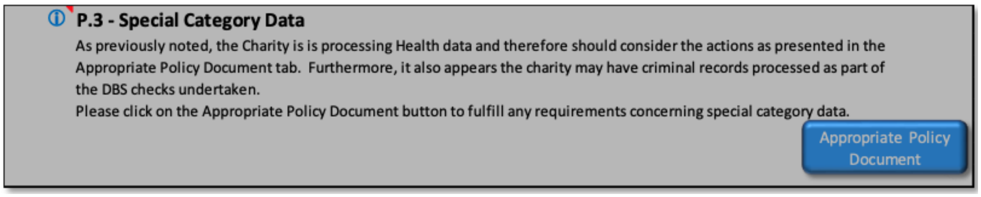


Observations from the Data Collection and Workflow Page

Based on the response from D.5.d you are processing credit card payments, compliance checks regarding PCI DSS are outside the scope of this document (although many privacy disciplines still apply) We also noted from the responses given in D.2.j and D.2.k you appear to be responsible for Special Category data. Furthermore, from the responses provided in D.5.c and D.7.c the charity is collecting explicit consent for the purpose of marketing.

Please note, if any of the above assumptions are incorrect, double-check your previous responses.

Figure 10. Observations example from workflow Tab (1).

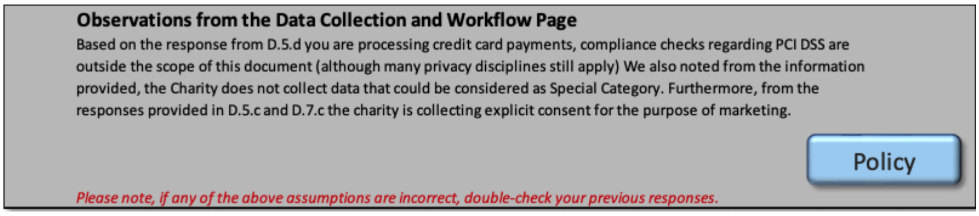


ⓘ **P.3 - Special Category Data**

As previously noted, the Charity is is processing Health data and therefore should consider the actions as presented in the Appropriate Policy Document tab. Furthermore, it also appears the charity may have criminal records processed as part of the DBS checks undertaken.

Please click on the Appropriate Policy Document button to fulfill any requirements concerning special category data.

Figure 11. Observations example from policy Tab (1).

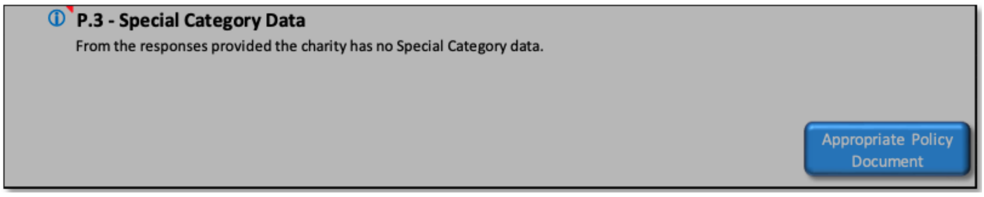


Observations from the Data Collection and Workflow Page

Based on the response from D.5.d you are processing credit card payments, compliance checks regarding PCI DSS are outside the scope of this document (although many privacy disciplines still apply) We also noted from the information provided, the Charity does not collect data that could be considered as Special Category. Furthermore, from the responses provided in D.5.c and D.7.c the charity is collecting explicit consent for the purpose of marketing.

Please note, if any of the above assumptions are incorrect, double-check your previous responses.

Figure 12. Observations example from workflow Tab (2).



ⓘ **P.3 - Special Category Data**

From the responses provided the charity has no Special Category data.

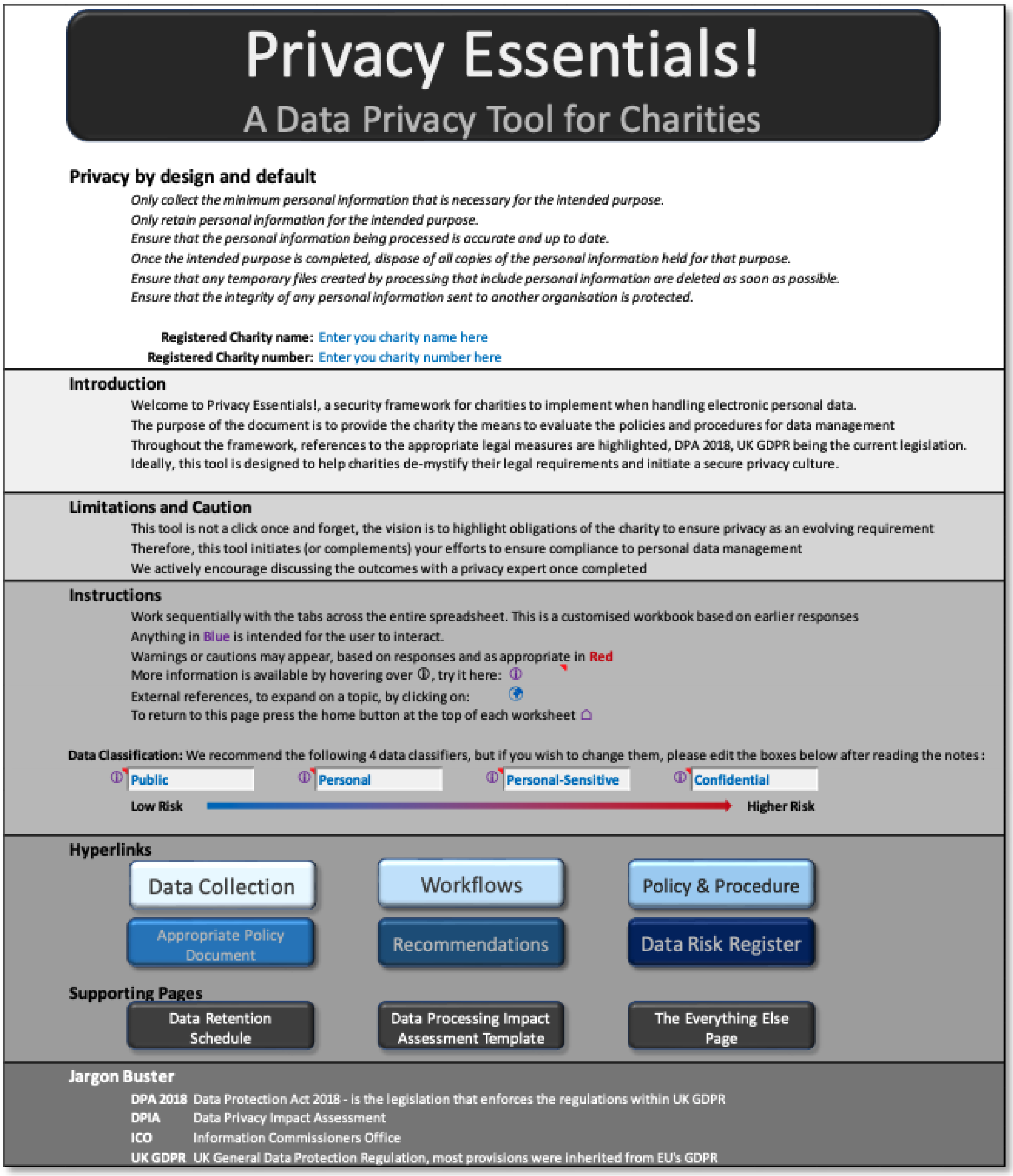
Figure 13. Observations example from policy Tab (2).

And in the case of Special Category data, further details are provided on the Policy Tab (Figure 11).

If D.2.j and D.2.k (Special Category) are changed to a negative response, the observation updates Figure 12.

Subsequently, this change is reflected in the Policy Tab in Figure 13.

Within PE, cells will be locked, and all calculations will be hidden on a separate tab so as to maintain the integrity of the worksheet as users enter their information. Access to all the tabs is presented with hyperlinks that will take the user to the next page for review or completion (Figure 14).



Privacy Essentials!
A Data Privacy Tool for Charities

Privacy by design and default

Only collect the minimum personal information that is necessary for the intended purpose.
Only retain personal information for the intended purpose.
Ensure that the personal information being processed is accurate and up to date.
Once the intended purpose is completed, dispose of all copies of the personal information held for that purpose.
Ensure that any temporary files created by processing that include personal information are deleted as soon as possible.
Ensure that the integrity of any personal information sent to another organisation is protected.

Registered Charity name: Enter you charity name here
Registered Charity number: Enter you charity number here

Introduction

Welcome to Privacy Essentials!, a security framework for charities to implement when handling electronic personal data.
The purpose of the document is to provide the charity the means to evaluate the policies and procedures for data management
Throughout the framework, references to the appropriate legal measures are highlighted, DPA 2018, UK GDPR being the current legislation.
Ideally, this tool is designed to help charities de-mystify their legal requirements and initiate a secure privacy culture.

Limitations and Caution

This tool is not a click once and forget, the vision is to highlight obligations of the charity to ensure privacy as an evolving requirement
Therefore, this tool initiates (or complements) your efforts to ensure compliance to personal data management
We actively encourage discussing the outcomes with a privacy expert once completed

Instructions

Work sequentially with the tabs across the entire spreadsheet. This is a customised workbook based on earlier responses
Anything in Blue is intended for the user to interact.
Warnings or cautions may appear, based on responses and as appropriate in Red
More information is available by hovering over ⓘ, try it here: ⓘ
External references, to expand on a topic, by clicking on: 🌐
To return to this page press the home button at the top of each worksheet ⌂

Data Classification: We recommend the following 4 data classifiers, but if you wish to change them, please edit the boxes below after reading the notes:

ⓘ Public ⓘ Personal ⓘ Personal-Sensitive ⓘ Confidential

Low Risk → Higher Risk

Hyperlinks

Supporting Pages

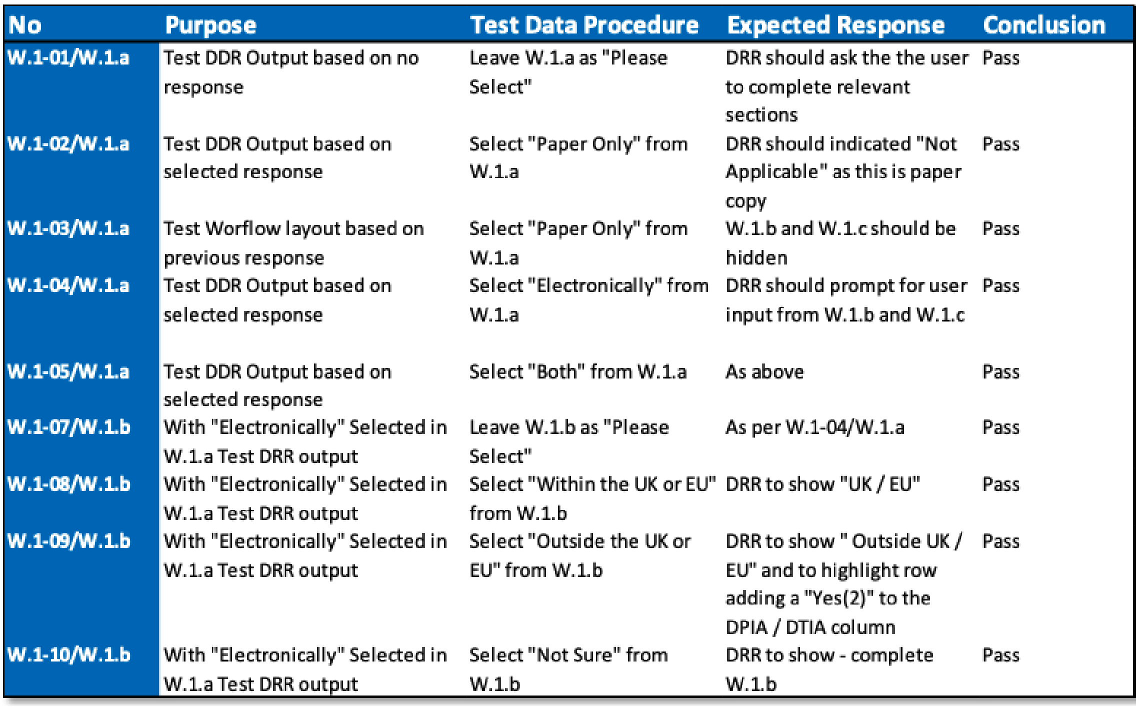
Jargon Buster

DPA 2018	Data Protection Act 2018 - is the legislation that enforces the regulations within UK GDPR
DPIA	Data Privacy Impact Assessment
ICO	Information Commissioners Office
UK GDPR	UK General Data Protection Regulation, most provisions were inherited from EU's GDPR

Figure 14. Privacy Essentials! welcome screen.

5.5. Black-Box-Style Testing

The research developer conducted black-box testing throughout the build as each section was completed. Following a dynamic bottom–up approach, evaluating each response and validating the outcome was as expected [59]. This allowed the developer to control the inputs in both the data collection and workflow screens, through either tick boxes, variable drop menus, or cell validation, thereby reducing the opportunity for user input error. Thus, in conducting these black-box tests, it was the functionality of the output that was assessed against expectations (see Figure 15 for an example).



No	Purpose	Test Data Procedure	Expected Response	Conclusion
W.1-01/W.1.a	Test DDR Output based on no response	Leave W.1.a as "Please Select"	DRR should ask the the user to complete relevant sections	Pass
W.1-02/W.1.a	Test DDR Output based on selected response	Select "Paper Only" from W.1.a	DRR should indicated "Not Applicable" as this is paper copy	Pass
W.1-03/W.1.a	Test Worflow layout based on previous response	Select "Paper Only" from W.1.a	W.1.b and W.1.c should be hidden	Pass
W.1-04/W.1.a	Test DDR Output based on selected response	Select "Electronically" from W.1.a	DRR should prompt for user input from W.1.b and W.1.c	Pass
W.1-05/W.1.a	Test DDR Output based on selected response	Select "Both" from W.1.a	As above	Pass
W.1-07/W.1.b	With "Electronically" Selected in W.1.a Test DRR output	Leave W.1.b as "Please Select"	As per W.1-04/W.1.a	Pass
W.1-08/W.1.b	With "Electronically" Selected in W.1.a Test DRR output	Select "Within the UK or EU" from W.1.b	DRR to show "UK / EU"	Pass
W.1-09/W.1.b	With "Electronically" Selected in W.1.a Test DRR output	Select "Outside the UK or EU" from W.1.b	DRR to show " Outside UK / EU" and to highlight row adding a "Yes(2)" to the DPIA / DTIA column	Pass
W.1-10/W.1.b	With "Electronically" Selected in W.1.a Test DRR output	Select "Not Sure" from W.1.b	DRR to show - complete W.1.b	Pass

Figure 15. Example black-box test.

PE was also tested for functionality independently. These tests proved successful, despite some date issues (potentially regional settings which could not be replicated). In addition, testing was also carried out on the functionality of the policies and procedures page, using similar black-box techniques, and that page worked as expected.

Following these successful tests, PE was submitted for evaluation to the client (Section 4), the other two charities that agreed to participate, and the Expert Advisor (Section 4.3.1) that had assisted earlier in the development phase (Section 5.2). For each of the client evaluations, the same testing regimes were followed for each improvement implemented.

6. Evaluation

To evaluate the usability, a meeting was set up with the client to demonstrate PE. This meeting took place via a 2.5 h video conference call, with feedback recorded as it was received. The other charities were sent copies of Privacy Essentials! and asked to provide feedback via a questionnaire as well as providing any ad hoc critique (Section 6.1).

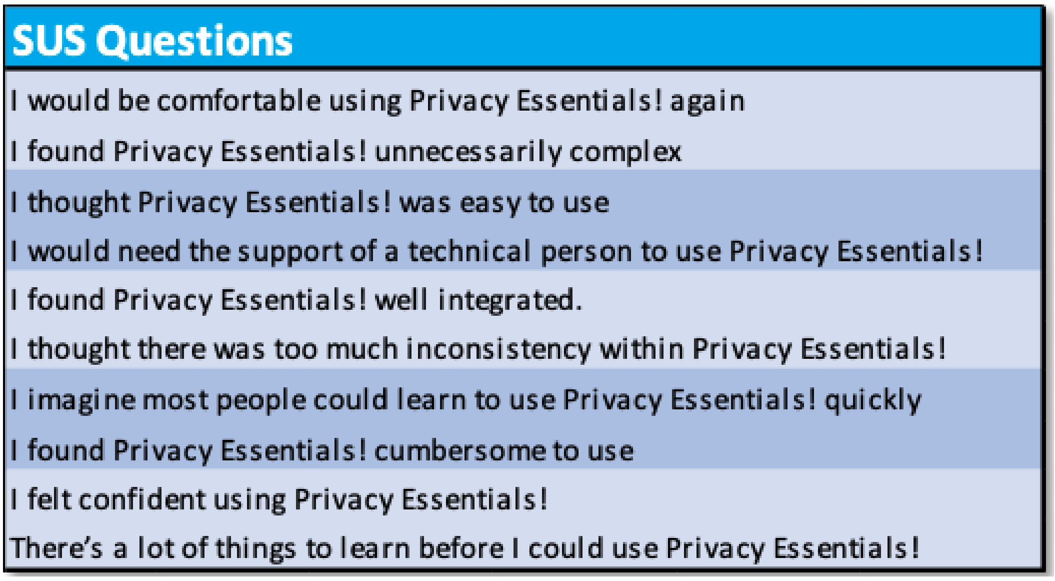
The final evaluation was conducted with a qualified DPO for a large charitable organisation to affirm that the functionality meets the intended markets' requirements. This DPO is also a Trustee for a charity with 140 locations across the UK, and therefore has an additional interest in the capabilities of Privacy Essentials!.

6.1. System Usability Survey

The System Usability Scale (SUS) [48] provides a useful insight into the usability of an application. It contains ten questions, with users responding on a 5-point Likert scale (ranging from Strongly disagree to Strongly agree).

This questionnaire was adapted for PE, and evaluators were asked to complete the ten questions (Figure 16), via an online survey (hosted by Jisc Online Surveys [60]); eight responses were received.

We plotted the individual scores against a spider graph and plotted the 'ideal score' in orange and our results from the PE SUS questionnaire shown in blue (Figure 17).



SUS Questions
I would be comfortable using Privacy Essentials! again
I found Privacy Essentials! unnecessarily complex
I thought Privacy Essentials! was easy to use
I would need the support of a technical person to use Privacy Essentials!
I found Privacy Essentials! well integrated.
I thought there was too much inconsistency within Privacy Essentials!
I imagine most people could learn to use Privacy Essentials! quickly
I found Privacy Essentials! cumbersome to use
I felt confident using Privacy Essentials!
There's a lot of things to learn before I could use Privacy Essentials!

Figure 16. SUS questions.

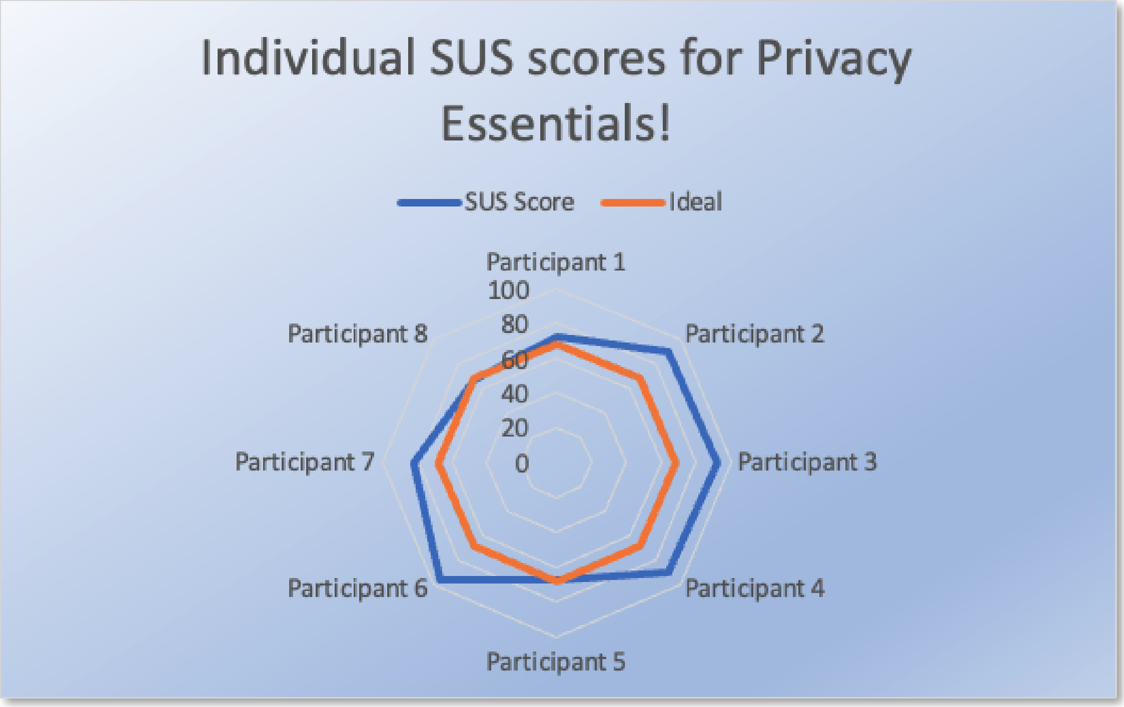
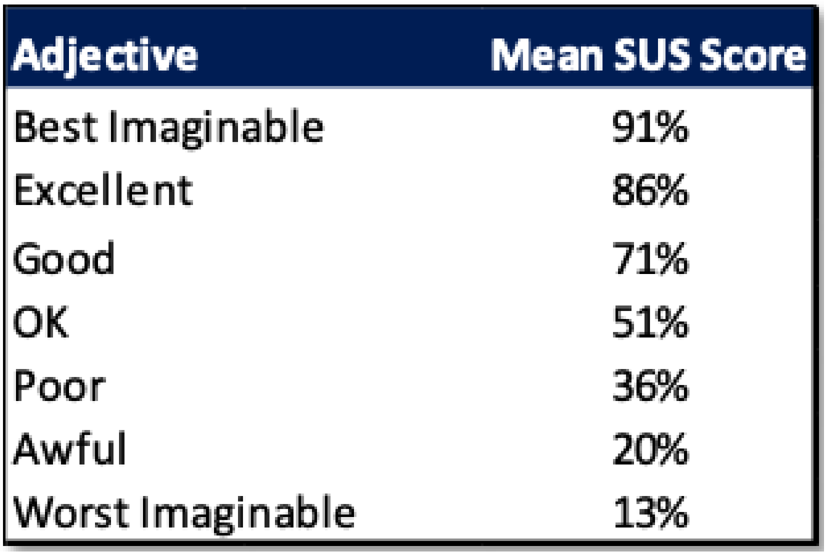


Figure 17. SUS results compared to ideal.

From this, the results suggest that users found PE intuitive to use. According to Brooke [48], a score of 68% is an average score, and anything above this is deemed acceptable. As regards the number of respondents, the optional number of respondents is thought to be between 8 and 12 [61]. Thus, we had eight evaluators completing the survey, who gave PE an average score of 82.2%; when compared against the SUS Adjective table shown in Figure 18, PE achieves a rating of "Good", approaching Excellent".



Adjective	Mean SUS Score
Best Imaginable	91%
Excellent	86%
Good	71%
OK	51%
Poor	36%
Awful	20%
Worst Imaginable	13%

Figure 18. SUS adjective table.

6.2. Evaluator Feedback and Improvements

One area of potential concern was whether the other two evaluated charities' needs could be assumed to be similar to those of the primary client. This concern was alleviated with evaluators responding to clarify that the identities and workflows in PE were equally appropriate to their operations. One point raised by Participant 5 (P5) was that the use of the word "Beneficiary" within PE could potentially cause confusion if PE was rolled out to other industries or sectors. Charities will use the term "Beneficiary" to indicate the identity of the recipient of the charity's services, which could potentially be misconstrued in other sectors. To alleviate this, this term could, however, be changed to "Client" to be more meaningful across other sectors.

Evaluators were also asked if there was any additional feedback for Privacy Essentials!; the responses, suggestions and changes applied in response to the feedback are depicted in Table 12.

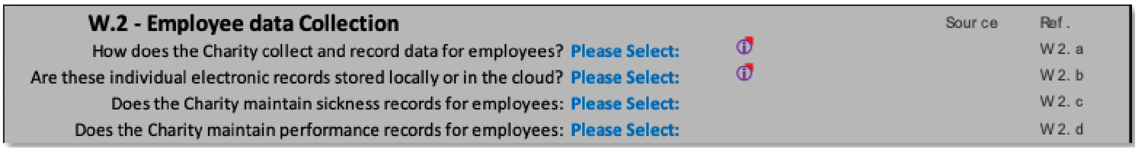
Table 12. Privacy Essentials! evaluation v1.0 feedback considerations.

Evaluator	Design Feedback	Resolution
P1	Truncated notes	Solution : Check each note and re-size to fit the contents
P2	Yes/No response to use linked tick boxes not a drop-down menu	Linked cells will have one box selected and the other not, the intention being to force a Yes/No response. Solution: leave as is
P3	Jump to next field useful	If user input was not forced, "Enter" jumps to the next cell —because of drop-down menus and tick boxes—next field is not automated. Solution: Leave as is, HTML version should fix this
P3	Other box in Data Collection should be white to indicate completion	Data Validation "hides" the row based on earlier response; however, a shadow of the "other" box would remain, potentially causing confusion. Solution: to leave as is and await further feedback
P3	Retention schedule should have an override for statutory requirements	It can be overridden today; however, the user wanted to retain the original value to show it was over-ridden (the notes do record the original limits). Solution: to leave as is and await further feedback
P3	Terminology "SaaS" unclear	Solution: Change SaaS to "Cloud" in the drop-down menus as that
P5	Terminology "Beneficiary" unclear	Solution: Keep as Beneficiary for the present, adapt to Client if feedback shared amongst other industries or sectors
P4	Tick boxes do not align on a Mac	Tick boxes were aligned using Excels Page Layout alignment—Quirk on a Mac? Solution: Alignment checked and snapped to "Centre"

Table 12. *Cont.*

Evaluator	Design Feedback	Resolution
P1	More colourful background	Potentially a future improvement.
P5	The Blue Text appears Purple	Microsoft have three “Blues” in their standard colours “Light Blue” looks washed out, “Blue” is the colour used or “Dark Blue”. Solution: Change the description to “Blue/Purple”?
P5	Ranking of Data Classification—could be misleading	Solution: remove the Low Risk–High Risk arrow, potentially re-order the list in the drop-down menu.
P2	Clipped text in headings (Retention Periods)	This can be improved—the developer wanted to use a combo box that requires Macros and is out of scope for this iteration.
Evaluator	**Functional Errors/Improvements**	**Resolution**
P6	Consent message shows despite no box being ticked under marketing	Solution:: Formula corrected to show nothing if marketing is not “Yes” —Potential to remove D.5.c, as this might confuse.
P7	Add an “Other” to security controls	Solution:: Expand cell selection to show all rows needed.
P6	“Health” information showing in P.3 despite unchecked “Health” boxes from Data Collection	Have been unable to replicate the error—if sickness records are collected in workflows, this will trigger the same warning. Solution: Test again and await other feedback.
P2	Treatment of Paper records	Future consideration-it is out of scope for this iteration
P2	Opportunity to add data owner names to the appropriate sections	Under consideration—medium-sized charities. This has the potential to be a useful function.
P2	Show only the sections that are needed.	Solution:: This is possible, and can be delivered with Macros—although within the capability of the researcher, out of scope for this project.
PE1	Add Information Security Management System (ISMS) documentation	Under consideration as potentially “project creep” but equally has the potential to be “too generic” and requires appropriate customisation

The data risk register (DRR) required further information from the Workflow page to enhance Article 30 documentation as previously shown in Table 6 in Section 2.2. Thus, we updated the questions for each identity as depicted in Figures 19 and 20.

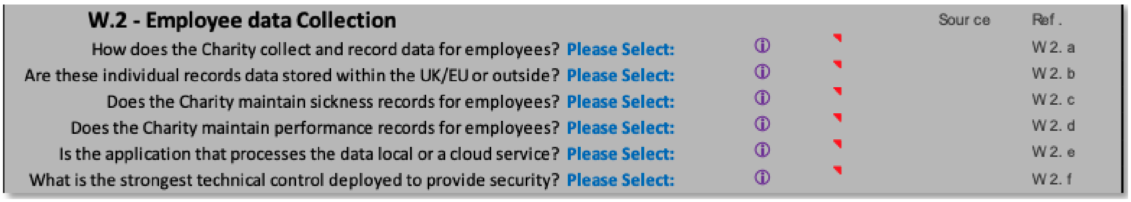


W.2 - Employee data Collection

			Source	Ref.
How does the Charity collect and record data for employees?	Please Select:	ⓘ		W2.a
Are these individual electronic records stored locally or in the cloud?	Please Select:	ⓘ		W2.b
Does the Charity maintain sickness records for employees:	Please Select:			W2.c
Does the Charity maintain performance records for employees:	Please Select:			W2.d

Figure 19. Privacy Essentials! v.1.0 Workflow page.

Looking at Figure 19, Ref. W.2.b was changed to be more meaningful to account for the relevance of the location of the stored personal data, with response choices presented now showing as “Within the UK/EU”, “Outside the UK/EU”, or “Not Sure”. Similarly, for Ref. W.2.e, responses, while similar, questioned the location of the application processing the data as opposed to the location of the data. Finally, W.2.f asks for the strongest security control, and although it could be argued that this question would be better served by a combo box, because PE is macro free, fields are limited to one response; therefore, this was left unchanged.



W.2 - Employee data Collection

			Source	Ref.
How does the Charity collect and record data for employees?	Please Select:	ⓘ		W2.a
Are these individual records data stored within the UK/EU or outside?	Please Select:	ⓘ		W2.b
Does the Charity maintain sickness records for employees?	Please Select:	ⓘ		W2.c
Does the Charity maintain performance records for employees?	Please Select:	ⓘ		W2.d
Is the application that processes the data local or a cloud service?	Please Select:	ⓘ		W2.e
What is the strongest technical control deployed to provide security?	Please Select:	ⓘ		W2.f

Figure 20. Privacy Essentials! v.2.0 Workflow page.

A caution was incorporated within the instructions to explain that the DRR can be manually enhanced to allow for scenarios where multiple applications are used to manage employee data. A feature that will permit more than one application to be recorded and automatically update the DRR may be incorporated in future iterations of PE.

6.3. UX Honeycomb Survey

After the amendments outlined in Table 12 had been implemented, a final evaluation of Privacy Essentials! v2.0 took place with the DPO introduced in Section 6 and the Client's CFO. For this, we used the UX Honeycomb survey [62] to obtain a qualitative assessment of Privacy Essentials! against seven variables as depicted in Figure 21.

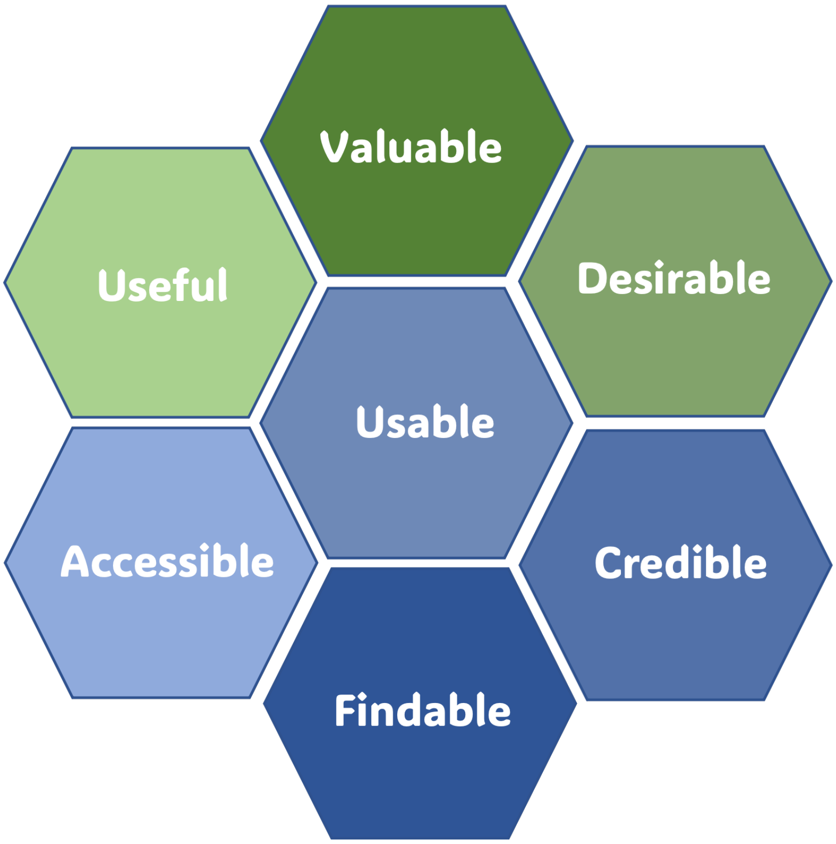


Figure 21. UX Honeycomb survey outcomes (adapted from [62]).

The UX Honeycomb survey was used to determine the appropriateness of the outcomes from PE v.2.0 using the seven questions listed in Table 13.

Table 13. UX Honeycomb questions.

ID	Questions
1	Was Privacy Essentials! useful to you?
2	Did you find Privacy Essentials! intuitive and were you able to process your requirements easily?
3	Did you find Privacy Essentials! desirable and did it meet your expectations?
4	Was it easy for you to find the information and features you needed to complete the task?
5	Was Privacy Essentials! accessible to you, were you able to use it without any issues?
6	Did you find Privacy Essentials! credible, did you trust the information and resources it provided?
7	Did you find Privacy Essentials! valuable, did it provide value for the time you invested in using it?

The responses received from the evaluators are shown in Table 14.

Table 14. UX Honeycomb evaluation responses.

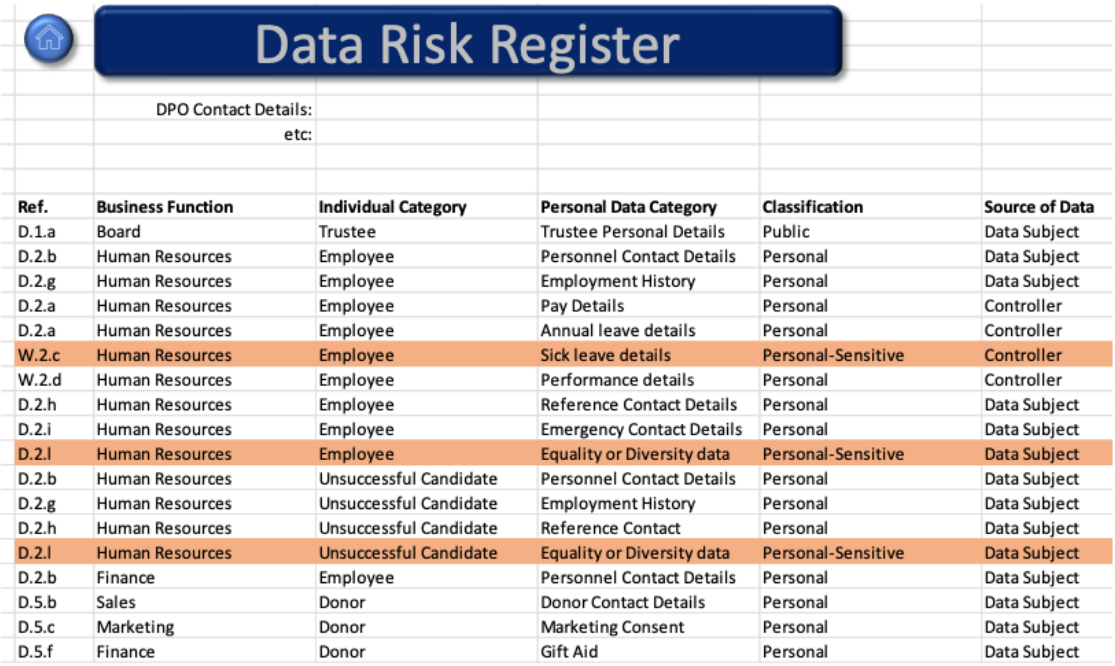
Question No./Evaluator	Response
1	**Was Privacy Essentials! useful to you?**
CFO	"We have not used it in a real situation yet, but having done a quick run through, I believe that it will be very useful to us."
DPO	*"Yes, as a data protection officer, I could easily relate to the questions being asked, why they were being asked, and how those responses may prompt action. I could envision various scenarios whereby this would be useful tool to sit down with individuals and use or refer to."*
2	**Did you find Privacy Essentials! intuitive and were you able to process your requirements easily?**
CFO	*"As always, at this initial stage of review, I found it comparatively easy with only a few issues with definitions."*
DPO	*"Yes, I was able to quickly work through the questions and view to the recommendations and data risk register in an efficient manner. I found many of the questions being limited to 'yes/no' or a list of possible answers extremely helpful. The recommendations and risk register were clear and would be useful to many stakeholders, including the ICO, should a charity ever need to provide evidence of their compliance posture."*
3	**Did you find Privacy Essentials! desirable and did it meet your expectations?**
CFO	*"Looking at what was presented to us and my initial use of it, I think that it is going to be a very helpful tool."*
DPO	*"It exceeded my expectations. I have had access to similar commercial off-the-shelf examples before; this is able to compete, if not beat those in terms of competition. A lot of thoughts have gone into what is required by data protection law/ regulation and what is expected as good practice but also the users' need in terms of very simple questions, in which, depending on the response, prompts action."*
4	**Was it easy for you to find the information and features you needed to complete the task?**
CFO	*"Other than a few comprehension issues with terms used and also clarity on when our organisation had both. The tool assumed that you had one or another but not both. Can get around it but doing it again with the other option."*
DPO	*"Yes, it was. It was helpful that I could jump ahead and back using the tabs. This suits my approach to working. I like to be able to explore and see what is being asked of or expected ahead of being asked. This tool enables that. Some platforms I have used has been very restricted in the journey the user has to take. Often requiring users to re-do or back track through menus"*
5	**Was Privacy Essentials! accessible to you, were you able to use it without any issues?**
CFO	*"It was accessible to me, but in the short time I used it I had a few minor issues – see above"*
DPO	*"No issues at all-found it very easy to use. The only times I encountered an issue I found it to be user error, I was jumping ahead and not reading the guidance note."*
6	**Did you find Privacy Essentials! credible. Did you trust the information and resources it provided?**
CFO	*"It does appear to be very credible"*
DPO	*"Yes, I can see a lot of thought, time and research has gone into looking for information that would be relevant and useful for the intended users."*
7	**Did you find Privacy Essentials! valuable, did it provide value for the time you invested in using it?**
CFO	*"Very much so"*
DPO	*"Yes, extremely valuable. I would not hesitate it recommending this to a charity who had the appetite and capacity to perform a review of their data protection/privacy posture. Such a framework would undoubtedly be of great value to them."*

Thus, from the results from the Honeycomb evaluation survey and our subsequent conversations with the evaluators, their responses were highly encouraging, and the comment of the DPO, "I have had access to similar commercial off-the-shelf examples before, this is able to compete, if not beat those in terms of competition", would indicate that PE more than meets the expected outcomes.

6.4. Privacy Essentials! v2.0 Improvements

Following feedback received from the v.2.0 reviews (Section 6.3), some minor improvements will need to be considered. For example, workflows could benefit from having additional processes included, with, for instance, drop-down menus that gather information about data locations, the likely lawfulness for processing, data retention schedules, and security treatments. Adding these would add further complexity to the framework, but in turn, would allow the DRR to capture richer data. However, keeping PE relatively simple in the first instance will build confidence for the novice user, and therefore, there is a fine balance to be struck.

Another enhancement will be Subject Access Request (SAR), where data will be added to the DRR, following the logic that, if either SAR policy, or procedure, is selected by the user, then the DRR will automatically add relevant fields. Similarly, if a Data Transfer is required, the DRR will highlight those requirements in a similar fashion to the way DPIA obligations are shown in Figure 22.



Data Risk Register

DPO Contact Details:
etc:

Ref.	Business Function	Individual Category	Personal Data Category	Classification	Source of Data
D.1.a	Board	Trustee	Trustee Personal Details	Public	Data Subject
D.2.b	Human Resources	Employee	Personnel Contact Details	Personal	Data Subject
D.2.g	Human Resources	Employee	Employment History	Personal	Data Subject
D.2.a	Human Resources	Employee	Pay Details	Personal	Controller
D.2.a	Human Resources	Employee	Annual leave details	Personal	Controller
W.2.c	Human Resources	Employee	Sick leave details	Personal-Sensitive	Controller
W.2.d	Human Resources	Employee	Performance details	Personal	Controller
D.2.h	Human Resources	Employee	Reference Contact Details	Personal	Data Subject
D.2.i	Human Resources	Employee	Emergency Contact Details	Personal	Data Subject
D.2.l	Human Resources	Employee	Equality or Diversity data	Personal-Sensitive	Data Subject
D.2.b	Human Resources	Unsuccessful Candidate	Personnel Contact Details	Personal	Data Subject
D.2.g	Human Resources	Unsuccessful Candidate	Employment History	Personal	Data Subject
D.2.h	Human Resources	Unsuccessful Candidate	Reference Contact	Personal	Data Subject
D.2.l	Human Resources	Unsuccessful Candidate	Equality or Diversity data	Personal-Sensitive	Data Subject
D.2.b	Finance	Employee	Personnel Contact Details	Personal	Data Subject
D.5.b	Sales	Donor	Donor Contact Details	Personal	Data Subject
D.5.c	Marketing	Donor	Marketing Consent	Personal	Data Subject
D.5.f	Finance	Donor	Gift Aid	Personal	Data Subject

Figure 22. Privacy Essentials!—DRR/Article 30 Page.

7. Conclusions

This paper has presented the Privacy Essentials! framework, a data protection assessment tool that will allow charitable organisations to begin creating and implementing an effective data privacy programme.

Identifying a gap in the market, our research found that charities have a tendency to struggle a little more than other sectors in being privacy and cyber savvy in their processes and practices, particularly smaller charities (Sections 1 and 2). One of our main contributions is the addressing of this gap. For this aim, we created a data protection assessment tool that will allow charitable organisations to begin creating and implementing an effective data privacy programme.

We achieved this through action research via working in close collaboration with three charities and two data privacy experts. This research has resulted in the main contribution of this paper, Privacy Essentials!, a step-by-step framework that charities can use to assess their privacy posture, and identify the steps they need to implement to establish a comprehensive data privacy programme.

Privacy Essentials! leverages existing privacy standards and guidance, such as the NIST Privacy Framework (Section 2.5.1), ISO 27701 (Section 2.5.2) and Cyber Essentials

(Section 2.5.3) and the legal obligations brought by the UK GDPR (Section 2.2), incorporating these to ensure charities cover all considerations around how best to manage privacy and handle data appropriately within the organisation. We coupled the insights gained from analysing these documents with primary data collected from the charities themselves through interviews and observation (Section 4) to create a series of Personas (Section 4.6.2) and requirements (Section 4.7).

From this, the logic and flow of Privacy Essentials was designed (Section 5), before using MS Excel to programme and create the actual framework itself (Section 5.4). Once we were satisfied that Privacy Essentials! worked as expected (Section 5.5), we went back to our collaborators and had them evaluate both v1.0 and v.2.0, and provide feedback on their findings (Section 6). To the best of our knowledge, the contribution of Privacy Essentials! presents a great opportunity for charities to gain privacy compliance.

Discussion and Future Work

Privacy Essentials! demonstrates how, with a little guidance and direction, an organisation can enhance their privacy posture. Coupled with the implementation of Privacy Essentials! recommendations, and building out the required policies, procedures, and processes, organisations can also build a solid foundation for their security programme.

The resulting privacy framework has been designed to guide practitioners through how to become privacy compliant, through a step-by-step decision tree framework that will output a pack of required documentation needed to satisfy UK GDPR compliance. One of the contributions of this paper is to make Privacy Essentials! freely available to the charity sector, and, should its adoption become possible within either the ICO or the Charity Commission, then their reach would allow the framework to be used by any of the 169,000 charities in the UK. For this aim, Privacy Essentials! can be accessed via the link provided here: https://eprints.bournemouth.ac.uk/39523/ (accessed on 1 January 2020).

Privacy Essentials! attempts to consider all personal data types and be as comprehensive as possible. One limitation is that certain data types that are unique (such as driving license or passport number) have been excluded. However, these can be accommodated within the framework under the heading classified as “other”. Similarly, Privacy Essentials! is limited to considering IT related matters, meaning the management of personal data on other media, such as social media, paper copies, video and audio, is not facilitated in this version of the framework. However, these may be added to this version of the framework as part of a future iteration.

A second limitation is that Privacy Essentials! limits the outcomes from processes of the Microsoft O365 licences due to time constraints around the study. Thus, the Google Suite was omitted deliberately. However, the processes as described within the framework will be equally applicable to Google, and the intention is that Privacy Essentials! will be updated to accommodate the Google Suite as part of future development.

Future work will seek to leverage the framework to be applicable to more industries and sectors. The disciplines required when protecting and managing personal data are readily transferable to other data assets, such as intellectual property, confidential information or any manner of sensitive documentation. We will also explore the opportunity offered by the DPO introduced in Section 6, who offered to potentially trial and further evaluate future iterations of Privacy Essentials! within the charity he is a Trustee of. This would allow Privacy Essentials! an opportunity to gain a wider audience to evaluate the framework and gather invaluable feedback, which is gratefully appreciated. To this end, further discussions are in progress at the time of writing this paper.

Author Contributions: Conceptualisation, J.T. and J.H.-B.; methodology, J.T.; software, J.T.; validation, J.T.; formal analysis, J.T.; investigation, J.T.; resources, J.T.; data curation, J.T.; writing—original draft preparation, J.T. and J.H.-B.; writing—review and editing, J.H.-B. and C.Y.; visualisation, J.T.; supervision, J.H.-B.; project administration, J.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Privacy Essentials! can be accessed via the link provided in Section 7.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CFO	Chief Financial Officer
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DRR	Data Risk Register
ICO	Information Commissioners Office
ISO	International Organisation for Standardisation
GDPR	General Data Protection Regulation
MoSCoW	Must have, Should have, Could have, Won't have
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
PE (PE!)	Privacy Essentials!
PECR	Privacy and Electronics Communication Regulation
SUS	System Usability Scale
UX	User Experience

Appendix A. Data Field Analysis

Table A1. New-volunteer request form.

Form Field	Personal	Sensitive	Unique	Comments
Recruiter Name	Yes	No	No	When coupled with other data, could identify the person
Recruiter Title	No	No	No	
Recruiter email	No	No	Yes/No	Publicly available information
Volunteer Office Address	No	No	No	Publicly available information
Postcode	Yes	No	No	Publicly available information
Home Phone Number	Yes	Yes	No	When coupled with other data, could identify the person
Mobile Phone Number	Yes	No	Yes *	* Mobile phones are normally used by a single individual-not shared
Advertised role	No	No	No	Publicly available information
Volunteer role	No	No	No	Publicly available information
Volunteer availability	Yes	Yes	No	Potential for criminality
Role title	No	No	No	Publicly available information
New Role	No	No	No	Publicly available information
Volunteer Required date	No	No	No	Publicly available information
Desired Skills	No	No	No	Publicly available information
Vehicle Access	No	No	No	
DBS	Yes	Yes	Yes *	* Dependant on past criminal records

Table A2. Marketing permissions form.

Form Field	Personal	Sensitive	Unique	Comments
Name	Yes	No	No	The entire form is personal data
e-mail	Yes	No	Yes	
Phone	Yes	No	Yes/No	
Postal Address	Yes	No	No	

Table A3. IT new starter form.

Form Field	Personal	Sensitive	Unique	Comments
Name	Yes	No	No	When coupled with other data, could identify the person
Title	No	No	No *	* If the title was Lord X, then potentially identifiable
Gender	No	Yes *	No	* Depends on the question asked
Date of birth	Yes	Yes	No	Popular authentication check
Address	Yes	No	No	Depends on the number of residents
Postcode	No	No	No *	* Postcodes are generally shared among many properties
Home Phone	Yes	Yes	No	When coupled with other data, could identify the person
Mobile Phone	Yes	No	Yes *	* Mobile phones are normally used by a single individual-not shared
Emergency contact	Yes	No	No	When coupled with other data, could identify the person
Contact number	Yes	No	No	
Availability	Yes	Yes	No	Potential for criminality
How did you discover the Primary Client?	No	No	No	
Reasons for volunteering	No	No	No	
Skills	Yes	No	No	
Personal benefit of volunteering	No	No	No	
Volunteer roles	No	No	No	
Access to a vehicle	No	No	No	
Criminal Offence	Yes	Yes *	Yes	* Dependant on past criminal records
Child abuse record	Yes	Yes *	Yes	* Dependant on past sanctions
Reference contact details	Yes	No	Yes	* Dependant on past criminal records
Signature	Yes	Yes *	Yes	Sensitive as potential for fraud

Table A4. Volunteer application/update form.

Form Field	Personal	Sensitive	Unique	Comments
Requested by	No	No	No	
Requested date	No	No	No	
Authorised by	No	No	No	Publicly available information
Start date	No	No	No	
First name	Yes	No	No	

Table A4. *Cont.*

Form Field	Personal	Sensitive	Unique	Comments
Last name	Yes	No	No	
Work email requested	Yes	No	No	
Job title	No	No	No	
Department	No	No	No	
Hours/Days working	No	No	No	No personal address shown
Office Address	No	No	No	Publicly available information
Office Phone	No	No	No	Publicly available information
Licence requirements	No	No	No	
AD Group permissions	No	No	No	
SharePoint ACL	No	No	No	
Notes	No	No	No	

References

1. Charity Commission for England and Wales. *Charity Commission Annual Report and Accounts 2021 to 2022*; Charity Commission for England and Wales: London, UK, 2022.
2. Verizon. *Data Breach Investigation Report 2008–2022*; Technical Report; Verizon: New York, NY, USA, 2022.
3. Klahr, D.R.; Shah, J.N.; Finnerty, K.; Chhatralia, K.; Rossington, T. *Cyber Security among Charities*; Technical Report; Ipsos MORI, on behalf Department for Digital Culture Media & Sport DCMS: London, UK, 2017.
4. Gneezy, U.; Keenan, E.A.; Gneezy, A. Avoiding overhead aversion in charity. *Science* **2014**, *346*, 632–635. https://doi.org/10.1126/science.1253932.
5. Ashford, W. Cyber Crime Is a Top Threat to UK Charities, Says NCSC. *Computer Weekly*, 2 March 2018.
6. Charities Aid Foundation. *UK Giving Report 2021*; Technical Report; Charities Aid Foundation: West Malling, Kent, UK, 2021.
7. Holgersson, J.; Kávrestad, J.; Nohlberg, M. Cybersecurity and Digital Exclusion of Seniors: What Do They Fear? In *The Human Aspects of Information Security and Assurance*; Furnell, S., Clarke, N., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 12–21.
8. European Parliament and the Council of Europe. General Data Protection Regulation (GDPR). In *Regulation (EU) 2016/679 5419/1/16*; European Parliament and the Council of Europe: Brussels, Belgium, 2016.
9. Abdullah, M.F.; Ahmad, K. The Mapping Process of Unstructured Data to Structured Data. In Proceedings of the 3rd International Conference on Research and Innovation in Information Systems—2013 (ICRIIS'13), Kuala Lumpur, Malaysia, 27–28 November 2013; pp. 151–155. https://doi.org/10.1109/ICRIIS.2013.6716700.
10. Blumberg, R.; Atre, S. The Problem with Unstructured Data. *DM Rev.* **2003**, *13*, 62.
11. *ISO 27001*; Controls—A Guide to Implementing and Auditing. IT Governance Publishing: Ely, UK, 2019.
12. *ISO/IEC 27701:2019*; Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management—Requirements and Guidelines. ISO: Geneva, Switzerland, 2019.
13. DCMS. *Cyber Security Breaches Survey 2018*; Technical Report; Department for Digital, Culture, Media & Sport (DCMS): London, UK, 2018.
14. ICO. *Data Protection Officers*; ICO: Wilmslow, UK, 2023.
15. Henriksen-Bulmer, J.; Faily, S.; Jeary, S. Implementing GDPR in the Charity Sector: A Case Study. In *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data, Proceedings of the 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, 20–24 August 2018*; Revised Selected Papers; Kosta, E., Pierson, J., Slamanig, D., Fischer-Hübner, S., Krenn, S., Eds.; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; Volume 547, pp. 173–188. https://doi.org/10.1007/978-3-030-16744-8_12.
16. Martin, N.; Matt, C.; Niebel, C.; Blind, K. How Data Protection Regulation Affects Startup Innovation. *Inf. Syst. Front.* **2019**, *21*, 1307–1324. https://doi.org/10.1007/s10796-019-09974-2.
17. Sirur, S.; Nurse, J.R.; Webb, H. Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). In Proceedings of the 2nd International Workshop on Multimedia Privacy and Security; Association for Computing Machinery,Toronto, ON, Canada, 15–19 October 2018; pp. 88–95. https://doi.org/10.1145/3267357.3267368.
18. Uchendu, B.; Nurse, J.R.C.; Bada, M.; Furnell, S. Developing a cyber security culture: Current practices and future needs. *Comput. Secur.* **2021**, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387.
19. Lloyd, G. The business benefits of cyber security for SMEs. *Comput. Fraud Secur.* **2020**, *2020*, 14–17. https://doi.org/10.1016/S1361-3723(20)30019-1.

20. Stokes, R. The Genesis of Banking Confidentiality. *J. Leg. Hist.* **2011**, *32*, 279–294. https://doi.org/10.1080/01440365.2011.627153.
21. Rothstein, M.A. The Hippocratic Bargain and Health Information Technology. *J. Law Med. Ethics* **2010**, *38*, 7–13. https://doi.org/10.1111/j.1748-720X.2010.00460.x.
22. Cram, I. *The Right to Respect for Private Life: Digital Challenges, a Comparative-Law Perspective-The United Kingdom | Think Tank*; European Parliament: London, UK, 2018.
23. *Data Protection Act 2018*; Queen's Printer of Acts of Parliament: London, UK, 2018. Available online: https://www.legislation.gov.uk (accessed on 22 April 2023).
24. Data Protection. 2023. Available online: https://www.gov.uk (accessed on 8 February 2023).
25. ICO. *For Organisations: UK GDPR Guidance and Resources: Data Protection Principles: Accountability Principle*; ICO: Wilmslow, UK, 2022.
26. ICO. *What Is a DPIA?*; ICO: Wilmslow, UK, 2022.
27. European Commission *ARTICLE29-Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)*; European Commission: Brussels, Belgium, 2017. Available online: https://ec.europa.eu/newsroom/article29/items/611236/en (accessed on 21 February 2023).
28. Radojev, H. ICO fines 11 major charities for data protection breaches. *Civil Society*, 5 April 2017.
29. Heiman, M.R.A. The GDPR and the Consequences of Big Regulation. *Pepperdine Law Rev.* **2020**, *47*, 945–954.
30. ICO. *UK GDPR Data Breach Reporting (DPA 2018)*; ICO: Wilmslow, UK, 2022.
31. ICO. *Guide to eIDAS Enforcement*; ICO: Wilmslow, UK, 2023.
32. Gibson, D.; Harfield, C. Amplifying victim vulnerability: Unanticipated harm and consequence in data breach notification policy. *Int. Rev. Vict.* **2022**, *29*, 341–365. https://doi.org/10.1177/02697580221107683.
33. Kuipers, S.; Schonheit, M. Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises. *Corp. Reput. Rev.* **2022**, *25*, 176–197. https://doi.org/10.1057/s41299-021-00121-9.
34. UK Parliament. *Data Protection and Digital Information Bill-Parliamentary Bills—UK Parliament*; UK Parliament: London, UK, 2023.
35. Fundraising Regulator. *Code of Fundraising Practice*; Technical Report; Fundraising Regulator: London, UK, 2019.
36. NIST. *About NIST*; NIST: Gaithersburg, MD, USA, 2009. Available online: https://www.nist.gov/about-nist (accessed on 21 February 2023).
37. Nadeau, E. *NIST Privacy Framework CORE*; Technical Report; National Institute of Standards and Technology (U.S.): Gaithersburg, MD, USA, 2020.
38. Harrington, D. U.S. Privacy Laws: The Complete Guide | Varonis. 2022. Available online: https://www.varonis.com/blog/us-privacy-laws (accessed on 21 February 2023).
39. ISO. *ISO Standards Are Internationally Agreed by Experts*; Technical Report; International Standards Office (ISO): Geneva, Switzerland, 2024.
40. *ISO/IEC 27701:2019*; An Introduction to Privacy Information Management. IT Governance Publishing: Ely, UK, 2020.
41. *ISO/IEC 27701*; Standard: Threats and Opportunities for GDPR Certification. ISO: Geneva, Switzerland, 2020. https://doi.org/10.21552/edpl/2020/2/7.
42. NCSC. *About Cyber Essentials*; Technical Report; National Cyber Security Centre NCSC: London, UK, 2023.
43. NCSC. *Cyber Essentials: Requirements for IT Infrastructure*; Technical Report v3.0; National Cyber Security Centre NCSC: London, UK, 2022.
44. Jayant.D, B.; Swapnaja, A.U.; Sulabha, S.A.; Dattatray, G.M. Analysis of DAC MAC RBAC Access Control based Models for Security. *Int. J. Comput. Appl.* **2014**, *104*, 6–13. https://doi.org/10.5120/18196-9115.
45. Government Security Classifications. 2018. Available online: https://www.gov.uk/government/publications/government-security-classifications (accessed on 14 February 2023).
46. McCallister, E.; Grance, T.; Kent, K.K.A.; National Institute of Standards and Technology (U.S.). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Draft): Recommendations of the National Institute of Standards and Technology*; Technical Report; National Institute of Standards and Technology (U.S.): Gaithersburg, MD, USA, 2009.
47. Eriksson, P.; Kovalainen, A. *Qualitative Methods in Business Research*; SAGE Publications Ltd.: London, UK, 2008. https://doi.org/10.4135/9780857028044.
48. Brooke, J. SUS: A Retrospective. *J. Usability Stud.* **2013**, *8*, 29–44.
49. Powell, R.A.; Single, H.M. Focus Groups. *Int. J. Qual. Health Care* **1996**, *8*, 499–504. https://doi.org/10.1093/intqhc/8.5.499.
50. ICO. *Documentation*; ICO: Wilmslow, UK, 2022.
51. Trites, G. Director responsibility for IT governance. *Int. J. Account. Inf. Syst.* **2004**, *5*, 89–99. https://doi.org/10.1016/j.accinf.2004.01.001.
52. Dai, C.; Barker, R. *Case Method Fast-Track: A RAD Approach*; Addison-Wesley: Boston, MA, USA, 1994.
53. Patton, J. *User Story Mapping*, 1st ed.; O'Reilly Media: Sebastopol, CA, USA, 2014.
54. Robertson, J.; Robertson, S. Volere-Requirements Specification Template. 2020. Available online: https://www.volere.org/templates/volere-requirements-specification-template/ (accessed on 12 April 2023).
55. Nielsen, J. 10 Usability Heuristics for User Interface Design. 1994. Available online: https://www.nngroup.com/articles/ten-usability-heuristics/ (accessed on 23 January 2023).

56. Loranger, H. Plain Language Is for Everyone, Even Experts. 2017. Available online: https://www.nngroup.com/articles/plain-language-experts/ (accessed on 18 February 2023).
57. Sears, A. *Human Factors and Web Development*; CRC Press: Boca Raton: FL, USA, 2003; pp. 21–46.
58. W3C. *Web Content Accessibility Guidelines (WCAG) 2.1*; Technical Report; World Wide Web Consortium W3C: Cambridge, MA, USA, 2018.
59. Nidhra, S. Black Box and White Box Testing Techniques-A Literature Review. *Int. J. Embed. Syst. Appl.* **2012**, *2*, 29–50. https://doi.org/10.5121/ijesa.2012.2204.
60. Taylor, J. Privacy Essentials! 2023. Available online: https://eprints.bournemouth.ac.uk/39523/ (accessed on 15 March 2024).
61. Tullis, T.; Stetson, J. A Comparison of Questionnaires for Assessing Website Usability. 2006. Available online: https://www.researchgate.net/publication/228609327_A_Comparison_of_Questionnaires_for_Assessing_Website_Usability (accessed on 3 April 2023).
62. Morville, P. Experience design unplugged. In Proceedings of the ACM SIGGRAPH 2005 Web Program; Association for Computing Machinery SIGGRAPH'05; New York, NY, USA, 31 July–4 August 2005; p. 10-es. https://doi.org/10.1145/1187335.1187347.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.