Kent Academic Repository

Bada, Maria, Furnell, Steven, Nurse, Jason R. C. and Dymydiuk, Jason (2023)
Supporting Small and Medium-sized Enterprises in using Privacy Enhancing Technologies. In: 5th International Conference on HCI for Cybersecurity, Privacy and Trust, 23-28 July 2023, Denmark. (In press)

Supporting Small and Medium-sized Enterprises in using Privacy Enhancing Technologies

Maria Bada[1] * [0000-0003-0741-5199], Steven Furnell[2][0000-0003-0984-7542],
Jason R.C. Nurse[3][0000-0003-4118-1680] and Jason Dymydiuk[1][0000-0003-3259-1709]

[1] Queen Mary University of London, London, UK
[2] University of Nottingham, Nottingham, UK
[3] University of Kent, Canterbury, UK
*Corresponding author
Maria.Bada@qmul.ac.uk; Steven.Furnell@nottingham.ac.uk; J.R.C.Nurse@kent.ac.uk;
J.Dymydiuk@qmul.ac.uk

Abstract. Small and Medium-sized Enterprises (SMEs) are a critical element of the economy in many countries, as well as being embedded within key and critical supply chains alongisde larger organisations. Typical SMEs are data- and technology-dependent, but many are nonetheless ill-equipped to protect these areas. This study aims to investigate the extent to which SMEs currently understand and use Privacy Enhancing Technologies (PETs), and how they could be supported to do so more effectively given their potential constraints in terms of understanding, skills and capacity to act. This was studied via a mixed method approach collecting qualitative and quantitative data. Survey responses from 239 participants were collected and 14 interviews conducted. Participants were SME owners as well as experts working with SMEs. The findings clearly demonstrate that SMEs generally tend not to think about privacy, and if they do so it is mainly because of risk, potentially after a cyber attack, with the main drivers for implementing privacy being the potential of being fined by regulators, reputational damage, the demands of customers, and legal or regulatory compliance. The main reasons for the lack of attention are lack of skills and necessity. On this basis, the findings were taken forward to inform the initial design of an SME Privacy Starter Pack, which aims to assist SMEs in understanding that privacy and PETs are relevant to them and their industry in a simple and facilitated manner.

Keywords: Small business, SMEs, Privacy, PETs, Data protection.

*** *This paper will be published at The 5th International Conference on HCI for Cybersecurity, Privacy and Trust (HCI-CPT 2023), at The 25th International Conference on. Human-Computer Interaction*

1 Introduction

Small and Medium-sized Enterprises (SMEs) are a critical element of the economy in many countries, as well as being embedded within key and critical supply chains with

larger organisations. Typical SMEs are data- and technology-dependent, but many are nonetheless ill-equipped to protect these areas. Very little is definitively known about their security strategies and day-to-day security challenges [1], but they are frequently viewed as easy targets by attackers [2]. Indeed, there is clear evidence to suggest that SMEs face a corresponding share of privacy incidents and data breaches [3]. At the same time, the challenges of understanding privacy and applying appropriate measures can be significant. For example, SMEs often do not fully appreciate the importance of the threats they can face and are limited in the attention that these can be given due to the need to maintain day-to-day business operations. Prior research has indicated that many struggle to engage even with conducting privacy impact assessments [4].

Organisations and users face numerous occurrences of privacy incidents and data breaches. In many cases, the challenges of understanding privacy and applying appropriate measures can be significant. SMEs often face numerous occurrences of privacy incidents and data breaches [5]. However, as owners and staff are immersed in day-to-day activities they may lack the time or expertise to fully understand the importance of, and protect themselves against, privacy threats. The Cisco Data Privacy Benchmark Study 2023 [6] clearly illustrates the importance of privacy for organisations globally. The findings of the report show that: most organisations say they need to do more to reassure customers about how their data is used; global providers are better able to protect their data compared with local providers; and all their employees need to know how to protect data privacy. Our study aims to understand more about the situation facing SMEs and seeks to provide additional support to help them move forward with greater understanding and confidence. Specifically, it investigates:

- the extent to which SMEs currently understand and use Privacy Enhancing Technologies (PETs); and
- how they could be supported to do so more effectively given their potential constraints in terms of understanding, skills and capacity to act.

This research has led to the initial design and development of an SME Privacy Starter Pack (SPSP) aiming to: a) promote awareness about privacy tailored to the unique needs of SMEs, companies with fewer than 250 personnel; b) support SMEs in identifying how privacy may relate to them (targeted at the organisational level but also guidance provided at an employee level) and how it plays a critical role in determining long-term performance and competitiveness; and c) develop a series of case studies and scenarios that will provide practical guidance to SMEs in order to identify which privacy harms and concerns are most important to them (e.g., these may be based on the types of privacy threats, relevant regulations and technologies already being used). The resulting guidance aims to assist all SMEs in understanding that privacy and privacy enhancing technologies are relevant to them and their industry in a simple and facilitated manner. The resulting value of the work is the development of new ways to engage with SMEs on privacy issues and enable them to improve their position. On a broader scale, it also offers a basis to build trust and to utilise privacy as a means to open a wider discussion on data protection and enhancing the cyber resilience of SMEs.

This paper begins with the literature review in this field. Following, an outline of the data collection methodology for interview and survey activities is presented in section

3, leading to discussion for the results obtained in each case in section 4. Section 5 then discusses how the findings help to inform the approach that has been taken in designing the proposed SME Privacy Starter Pack and presents the work to date on the associated prototype. Section six then highlights the coonclusions of this study.

2 Literature review

As context for the research undertaken with the SMEs, this section examines the related background in terms of the Privacy Enhancing Technologies (PETs), followed by tools and frameworks that have been established to support organisations in the pursuit of privacy issues, and finally the extent of specific support available to SMEs.

2.1 Privacy Enhancing Technologies

PETs have been characterised in various ways. Based on the work by Royal Society [7] PETs '*are an umbrella term covering a broad range of technologies and approaches that can help mitigate security and privacy risks*'. According to the Centre for Data Ethics and Innovation [8] PETs are '*any technical method that protects the privacy or confidentiality of sensitive information*'. This broad definition covers a range of technologies, from relatively simple ad-blocking browser extensions to the Tor network for anonymous communication. These set of technologies are divided in two categories: traditional and emerging PETs. Traditional PETs are well-established privacy techniques, such as encryption schemes that secure information in transit and at rest, and de-identification techniques such as tokenization and k-anonymity. Emerging PETs are a group of technologies that have begun to provide novel solutions to privacy challenges in modern data-driven systems. Primarily five technologies are considered: homomorphic encryption, trusted execution environments, secure multi-party computation, differential privacy, and systems for federated data processing.

ENISA [9] classified privacy enhancing technologies as the special type of technology tailored for supporting pseudonymous identity for data, anonymity or data and minimising data. The definition of ENISA also suggests that PETs have been tailored for supporting core data protection and privacy principles. Examples are: a) cryptographic algorithms: encryption; b) data masking techniques: pseudonymisation and c) with the help of AI & ML algorithms: data minimisation by reducing the amount of data that must be retained on a centralised server or in cloud storage.

Previous work from the Royal Society [7] sought to explain and scope some of the available PETs alongside their current development and potential through case studies and a sample of some technologies, that are ready for use and others in prototype phases.

Further work from ENISA [10] outlined the criteria required of online privacy tools in the aim of increasing trust and assurance in their use by the general public. ENISA divided them into three categories: basic, quality, and functionality. PETs are also frequently linked to the notion of Privacy by Design, because their development usually

implicitly takes into account some related principles, in particular privacy by default and end-to-end security [11], and more recently also respect for user privacy.

2.2 Frameworks and Tools with a Privacy Component

Having established that there are issues to be addressed, organisations need support and guidance in how to do so. A number of existing frameworks include components in relation to privacy. A representative set of these is discussed below.

ENISA defined the PETs control matrix [12], an assessment framework and tool for the systematic presentation and evaluation of online and mobile privacy tools for end users. The term 'PET' is used in the context of this work with a narrow focus, addressing standalone privacy tools or services (and not the broader concept of privacy enhancing technologies). In addition, the NIST Privacy Framework [13] can support organisations in: a) building customers' trust by supporting ethical decision-making in product and service design or deployment; b) fulfilling current compliance obligations, and c) facilitating communication about privacy practices with individuals, business partners, assessors, and regulators. More recently, the NIST Special Publication 800-53A [14] provides a methodology and set of procedures for conducting assessments of security and privacy controls employed within systems and organisations within an effective risk management framework.

The UK's ICO [15] has published an awareness campaign 'Think Privacy Toolkit' with training resources for businesses, providing messages about the importance of data and phishing, responsibility, reputation, and respect. However, it does not provide guidance on how to comply with GDPR and DPA 2018 or how to implement PETs. In addition, the Centre for Data Ethics and Innovation (CDEI) developed a PETs Adoption Guide [8]. The CDEI PETs Adoption Guide is a question-based flowchart to aid decision-makers in thinking through which of the PETs may be useful in their projects. The guide seeks to support decision-making around the use of PETs by helping the user explore which technologies could be beneficial to their use case.

In addition, a number of existing resources offer guidance and support such as the Reset the Net [16] resource which under the 'Privacy Pack', offers free software tools covering different privacy areas like instant messaging, anonymous browsing or email encryption, the Best Privacy Tools website [17] which offers help for preserving privacy online and the Internet Privacy Tools [18] a website that identifies some of the major areas of interest regarding the protection of private data and communications, such as encrypted email, file and disk encryption and wiping, anonymous browsing. Additionally, a concept of a tool [19] for the GDPR-compliant handling of person-al data by employees was created that supports employees in data management and data protection compliance. Also, AMBIENT Automated Cyber and Privacy Risk Management Toolkit [20] has been designed to be used in the healthcare domain for a variety of use case scenarios related to health data exchange.

ENISA [21] developed a tool on Privacy Enhancing Technologies (PETs) knowledge management and maturity assessment and provided recommendations on how to build and maintain an online community for PETs maturity assessments, which is assisted by ENISA's tool [22]. In addition, ENISA [23] developed a web application

prototype, the 'PET maturity assessment online repository' which supports the maturity assessment methodology by implementing a systematic collaborative process.

2.3 Existing Tools for SMEs

Various tools and guidelines have also been developed specifically targeting SMEs. Some relevant examples are presented and discussed below in order to give a sense of the resources available to those that look for it.

The ICO self assessment checklist [24] has been created with small business owners and sole traders in mind. The checklist provides information on how understanding data protection can increase a business's reputation, increase customer and employee confidence, and by making sure personal information is accurate, relevant and safe, save both time and money. Once an organisation completes the checklist a short report is created suggesting some practical actions SMEs can take and providing links to additional guidance for them to read that will help them improve their data protection knowledge and compliance.

The Global Cyber Alliance (GCA) [25] developed the GCA Cybersecurity Toolkit for Small Business, a free online resource simple, accessible and engaging that falls inro a cybersecurity trend of indirectly engaging in entry level privacy issues without acknowledgement.

ENISA [26] aimed to support SMEs, through practical guidelines on the security of personal data processing, on how to calculate the risks for personal data processing and adopt appropriate security measures. The approach undertaken is an attempt to bridge the gap between the legal provisions and SMEs understanding and perception of risk.

Sangani et al. [27] designed a framework that brings out a Security & Privacy Architecture as a service for SMEs (SPAaaS) pertaining to Web Applications which can be offered by various security vendors. SPAaaS aims to assist the SMEs to evaluate the security requirements pertaining to host their data and services on the cloud.

Although these tools and frameworks aim to support SME privacy practises they can quickly become complicated to follow, and often lack a direct recognition of Privacy Enhancing Technologies and potential benefits to SMEs. Additionally, privacy and PETs specific tools are often targeted at developers, those with prior knowledge, or more technical backgrounds in data processing. Therefore, the barriers to begin the process for novices and SMEs without technical officers are increased. They may need to invest in technical knowledge or in contracting companies greatly increasing the upfront cost. Another common gap is that the tools tend not to distinguish privacy from information security, leaving SMEs with a potentially confused message on the privacy-specific issues.

3 Methodology

Our main objective is to understand the drivers that SMEs have, and unique obstacles that they face, in making privacy-aware decisions (e.g., about actions, requirements, and technologies), and to subsequently provide a suite of support to aid them in

understanding and implementing appropriate PETs. To fulfil the above objectives, we collected qualitative and quantitative data using a mixed method approach [28]:

- Online survey (quantitative data): A survey was conducted to enable us to reach a wide sample of micro, small, and medium organisations. The results of the survey enabled us to collect data on the situation and understanding of privacy across different sectors.
- Interviews (qualitative data): The importance of the interviews was to gain an in depth understanding of what SMEs currently comprehend and what they actually need to know around privacy issues. This was achieved through interviewing different stakeholders such as SME owners as well as experts working with SMEs. We are supplementing this data with interviews conducted with persons involved in supporting SMEs through their information and privacy processes. Their understanding of the regulations and how to engage businesses and individuals, let alone getting them to act, means that they hold key information that can help to inform our findings and the subsequent the privacy starter pack.

Participants in this study were different stakeholders such as SME owners as well as experts working with SMEs. This includes third-party support SMEs – companies and personnel who help business meet regulation – as well as bodies that administer and assess certification schemes in the UK. Throughout the process of recruiting participants, data collection and analysis, all necessary steps to ensure anonymisation of data was followed. Personal information such as names were not collected or stored. Consent forms were collected prior to participation informing participants about the aim of the project and the data handling and storing process.

The participants of the online survey were given the opportunity to enter a raffle to win one of the three Amazon vouchers (£50 each) at the end of their participation. A separate survey was created to direct participants if they wished to participate in the Amazon voucher raffle. This ensured no contact details are linked to a specific survey response. Also, ethics approval for this project was granted from the Psychology Department Research Ethics Committee (Ref: PSY2022-41) at Queen Mary University of London and the National Research on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN) Ethics Board [29]. The latter being the funding body for this research.

4 Results

This section presents and discusses the main findings of the two data collection phases, focusing firstly upon the quantitative data from the survey, and then considering the accompanying qualitative insights from the interview sessions.

4.1 Quantitative Data

In total, 296 participants responded to the online survey. Of these, 239 responses were fully completed. The results are based on the complete 239 responses. The data

collected for the online survey are analysed producing descriptive statistics. A total of 36 questions comprised the online survey.

In terms of the role of the participants in their organisation, the majority are a programme manager (28%), researcher (23%) or in IT support (17%). In addition, 3% indicated a different role (Other) such as head of business unit, risk advisor or security assurance manager.
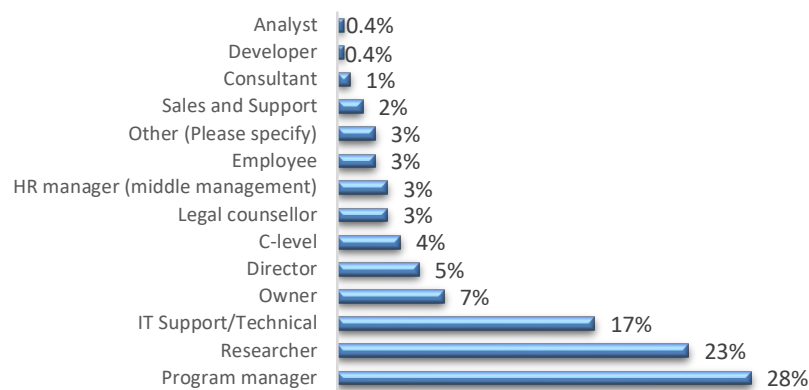

Fig. 1. Participant Role in Organisation (n=239)

The majority of organisations are a small (10-49 employes) (54%) or medium business (50-99 employes) (32%). In terms of the sector, participants mainly belong to an organisation focusing on Information Technology, professional scientific and technical activities, and public administration. The majority of participants claim that they somewhat consider privacy in their day-to-day business (40%), 25% responded that they do so very little, 21% not at all, while 14% to a great extent.

The main drivers for implementing privacy controls are: a) a perceived threat of losing an important customer (40%); b) gaining new business (21%); c) being part of the 'license to operate' perception (15%); d) the demands of customers (13%); e) compliance (8%); f) the potential for reputation damage (2%); g) the desire to avoid potential loss (1%). From what we observe, the majority of motivations are mainly customer-driven, either because they directly search for new customers, or because their business could be gained or lost because of losing existing ones.
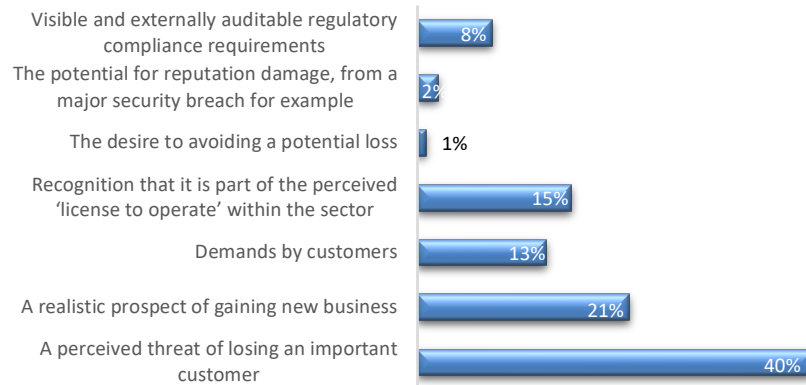
Fig. 2. Main drivers for implementing privacy – Multiple answer (n=239)

The main practises followed to keep data secure are: a) physical security measures (keeping documents secure in lockable storage) (51%); b) logging off computers when not at use (40%); c) encrypting mobile devices & use passwords (6%); d) using external storage devices (2%); e) back-ups (1%); f) other (0.4%) such as encrypting the data or using cloud services to retain data i.e. CRM. The results illustrate a lack of best practise use such as backing up data and using best practise for data encryption.

In addition, the majority of participants stated that privacy is an essential component of the overall strategy of their organisation, and they do have a data governance strategy as well. Also, most organisations consider privacy an essential component for developing a culture of accountability and responsibility. The results indicate that the majority of participants understand the distinction between personal and sensitive data and have a record of what personal data they hold, such as email addresses, names and medical information. In addition, participants know what personal data are used for and they only keep personal data for as long as it is needed.

In terms of being targeted by cybercriminals, most participants perceive their organisation as being an attractive target and have also been attacked in the past. However, the majority of participants consider that there would be very little harm in the event of a data breach. Lastly, participants mentioned that during internal exercises they would consider the cost of a data breach.

The main sources of information on privacy used by study participants are: a) the ICO (46%); b) ENISA (22%); c) Data Protection Officer (9%); d) NIST (6%); e) Federation of Small Businesses (FSB) (6%); f) legal department (5%); g) Information security colleagues (2%); h) professional training (2%); and i) Internet sources (1%). The results show that the ICO is a go-to platform for information and guidance for SMEs. However, the Federation of Small Businesses (FSB) [30], a UK business organisation representing small and medium-sized businesses offering a wide range of vital business services including advice, financial expertise, support, is a source less visited for privacy related information.

The main responsibility for privacy related decisions is placed upon the: a) CIO or equivalent (35%); b) CFO (20%); c) CISO (12%); d) data protection officer (8%); e) IT director (8%); f) CEO (6%); g) the departmental manager (5%); h) all employees (3%); and i) HR manager (2%). The results show that privacy related matters are mainly handled by the chief information officer (CIO) or the CFO (Chief Financial Officer). The CIO usually plays a key leadership role in the critical strategic, technical and management initiatives — from information security and algorithms to customer experience and leveraging data — that mitigate threats and drive business growth, while the CFO has substantial input into a company's investments, capital structure, money management and long-term business strategy. However, in the case of SMEs we often see the role of a Fractional Chief Information Officer (CIO) as a part-time executive who usually works for more than one primarily small- to medium-sized enterprise (SME) and develop promising avenues for future research on Fractional CIOs [31].

Participants were asked how they consider and discuss topics of privacy internally. Some of the responses collected indicate that usually such discussions will emerge during a Management Board, an Infosec Committee meeting or the biannual trainings. In addition, privacy would come into discussion during internal audits, bidding for work, or due to customer requirements. Some participants also mentioned that they would consider privacy requirements during the development of their products.

The majority of participants (86/%) were aware of PETs, 8% were not aware of PETs (34%), while 6% were not sure. From those organisations who are aware, the majority also engage with these practises. The main reasons for organisations not utilising PETs are the lack of a PET catalogue (43%), the requirements being covered by the internal implementation (29%), the lack of skills (14%) and the fact that PETs are not available for purchase by a 3rd party (14%). In addition, the majority of participants stated that they develop PETs in house based on reusable patterns. The main privacy tools used by participants are the GDPR (53%) and Fair Information Practice Principles (FIPPs) (25%).

In terms of decision-making processes followed when implementing PETs or making privacy related decisions, the majority of participants indicate that decisions are based on perceptions of leaders in the organisation (86%) but also they use external expert advice (35%). Additionally, internal expert advice (21%) and online resources (24%) are used to make such decisions. Participants seem to base their decision-making process less on using technology (11%) or on the support of internal support communities (1%). These results agree with the findings showing that privacy related decisions are usually made at a senior level within an organisation. It is also common for SMEs to ask for advice from an external consultant or search the Internet for related information.

Some of the challenges faced in relation to implementing PETs are: a) reusability issues (34%); b) the use of legacy projects (21%); c) lack of a PET catalogue (14%); d) the lack of detailed requirements (10%); e) difficulty in differentiating sensitive data (8%); f) high computational cost (4%); g) lack of training (2%); h) lack of resources or regulatory oversight (2%); i) the immaturity of implementations (2%); j) the difficulty to avoid sensitive data leakage (2%).

Finally, participants provided their suggestions for being best supported to use PETs. These are: a) provision of tools for implementing PETs (41%); b) the provision of clear instructions on how personal data may be processed (20%); c) provision of templates for data inquiries (13%); d) the use of a PETs catalogue (10%); e) the provision of clear requirements on obtaining personal data (8%); f) low computational cost (6%) and g) skilled employees (1%).

4.2 Qualitative Data

To complement the survey data, a series of 14 semi-structured interviews were conducted to explore the SME views and constraints in more detail. The interviews were audio-recorded, and transcriptions were then analysed using thematic analysis [28]. An iterative process was followed to first identify preliminary codes of the qualitative data collected. Then a further analysis was conducted to identify themes in our codes across the different interviews. These are collated and summarised as follows:

— **Perceptions and attitudes of SMEs about privacy:** According to interviewees, SMEs overall do not think about privacy and if they do it is mainly because of risk, potentially after an attack. Another interesting observation during interviews is that SMEs face the same risks and need to follow the same practices as larger organisations. However, the GDPR language is too difficult to understand. In addition, SMEs have a number of organisations telling them what to do, without necessarily explaining them why. Given the perception barriers around cybersecurity and technology, it was suggested that perhaps the best way to approach SMEs is by asking SMEs what they feel their most valuable assets are and whether they fell they need to protect these: '*We don't exist without data….Some small businesses have realised the issues and seek to be certified with Cyber Essentials'*. In addition, interviewees mentioned that people choose not to make privacy a priority, because there are other priorities, for which SMEs know what they need to do, know deadlines and know what will happen if they don't fulfil these. In terms of incentives, interviewees claimed that SME owners are also worried of being fined by the ICO. For this reason, they would follow a risk versus benefit approach. As an incentive, for SMEs it is suggested to promote that '*having Cyber Essentials will give you a lower fine'*. Supply chain expectations could also be another useful factor - i.e. that those using the SME as a supplier having an expectation of measures being in place.

— **Risk Perception:** According to interviewees, SMEs overall do not think that they are an attractive target for cybercriminals. As stated, '*I assume that organisations of high value would be a target. We don't have a lot of reserve in the bank. So we are not an attractive target. So, criminals would not attack us'*. It was further suggested that '*SMEs know that they might get in trouble with the ICO if they share data accidentally, but they don't know in how much trouble and they believe that by apologizing they will not be fined. And this impacts how they perceive risk'*. In addition, we have identified a sense of 'blind trust' from both clients and SME owners: '*Most of our clients trust us to be sensible. Similarly, we trust our developers to take measures so that we avoid an attack'*.

— **Information on PETs and use for SMEs:** Our findings indicate that forcing SMEs to meet best practices or in case of supply chains the practices of the lead, and often cyber mature, organisations is not effective. In addition, employing internal measures to meet frameworks such as ISO27000 is not feasible for many small companies that possess small budgets and minimal personnel. Because of this, organisations having SMEs in their supply chain ignore basic security requirements especially when it comes to SMEs. This has not only become apparent through our qualitative data collection but is also evident through the priorities of government agencies and their partnerships in academia – such as the National Cyber Security Centre and the Re-search Institute for Socio-Technical Cyber Security (RISCS) [32]. One interviewee stated that in the case of charities, advocacy, and the social clubs, such demands on smaller organisations to meet legislation and regulation could shut down the entire sector. The dream resolution would be a device set up to meet the requirements of privacy – encryption of resting data, access protocols such as 2FA, and timed notifications of data to ensure unnecessary data is not stored beyond requirement or a stated timeframe. Such a device would have a certified 'stamp of approval'.

— **Recognising constraints:** Another aspect which emerged in our interviews is the lack of focus on privacy due to many organisations being very small in size, which do not have someone working specifically on privacy. As mentioned by an interviewee '*We make use of 'pro bono' information and advice. This is how I became a member of the London Digital Security Centre….. It's like health and safety, people don't like to go to the authority, because they think that the authority is making them do more that they have to. This is why they are not looking at the information provided by the ICO'*. The first step, then, is toward basic practices, understanding and processes. Money is often key to the discussion and to the uptake of privacy in any business. Is it worth the cost? This brought up numerous discussions during the interviews revolving around regulatory fines, fine reduction systems (when a breach inevitably occurs), insurance, and tone of our privacy starter pack pitch – that is, it should not be demanding, but should be persuasive and helpful for SMEs to recognise why PETs are useful. Finally, SMEs and specifically for charities, information and advice is being sought through the official bodies '*there is the official body for each aspect such as the ICO for data, and then you can join a group such as the charity finance group, and you can find advice from such groups*'.

— **SMEs Privacy Starter Pack (SPSP) Specifications:** In relation to the development of the SPSP interviewees suggested the following: a) provide simple advice; b) prioritise 2-3 main basic steps SMEs need to follow; c) inform SMEs why it is important to follow best practise and privacy related guidance; and d) provide information in digital and physical form. In addition, interviewees suggested the SPSP to be designed in multiple accessible formats. First, to provide basic guidance, demonstrating to everyone that privacy is a concern to their business, no matter what sector. It would also include a section entitled: '*what to ask your…*' with questions to ask a cloud service provider, an accountant, payroll, or payment service provider on data protection. Second, provide guidance with core considerations with a focus on different sectors. This would have more sector specific questions and guidance. Our

initial results have already demonstrated that one-size approach is unlikely to fit all. This guidance too would include a '*questions to ask…*' section . However, unlike the above guidance, these would be aligned to a sector. Third, guidance on privacy and what SMEs might require. Interviewees also referred to the need for SMEs to understand why they need to consider privacy, how they need to consider it and clear channels for them to find useful advice. In terms of the approach '*Less is more. Everything you need to know is on the ICO website, but people don't have the time to go through all this information. It looks too complicated. You need to provide the top 5 priorities they need to do*'. And also '*Is there a clear path? If you can walk people through, you have a better chance*'. Telling stories about real people has been suggested as the beast approach. That would help because a lot of the time it is thought that the advice is for someone else, SMEs do not relate to that information or existing templates do not match to their needs. As stated, '*Templates, enough examples so that people can find something they can start with. You can find similar information, but it is different colour, you need to trick people into thinking that this is the right one*'.

The points from the latter theme feed into the next phase of the work, which is the design and development of a proposed Starter Pack to support SMEs in understanding and addressing their privacy needs (which in turn provides a foundation for their potential adoption of PETs).

5   Toward an SME Privacy Starter Pack

The findings from the quantitative and qualitative analysis conducted provided us with some basic understanding of current practices SMEs follow in relation to privacy. In addition, challenges and gaps have been identified which feed into the work towards the development of an SME Privacy Starter Pack (SPSP). Based upon the findings to date, such a tool is considered to require:

- **A tiered or level approach to encourage manageable and measurable steps**. Associating with the mind map the levels will work through an information audit where entry-level information security will be addressed incrementally rising to the recommendation of tools for adopting PETs for privacy requiring taskings as appropriate. Such an approach is key to increase the number of entry points into PETs to take into account existing information security or data handing knowledge.
- **Physical guide and resource**. Within the qualitative research phrase and interviews it became clear of the requirement to provide physical resources. Suggestions in the interviews included decision tables, templates, delegation packs, printer friendly information sheets, posters, and reports. In other words, taking into account the fact that each person has preferred learning style or condonation of kinetic, visual, and auditory.
- **Interactive, logged, and specific interface**. The information provided must be simple and accessible. Overwhelming displays or avenues of decision making might produce accurate results, but not at the cost of losing engagement. However, the starter pack, since it is incremental and bitesize requires adequate logging of the

decisions made for efficient adaptation as businesses and data processing of PII or sensitive information evolve. A likely aspect once the benefits beyond a decreased risk to processes already in place.

— **Relevant information matching the needs of SMEs.** Information that provides guidance that SMEs consider relevant and confident to use. Interviewees discussed the difficulty in deciding which information to use since there are multiple resources providing basic steps for organisations to ensure they protect their data. However, that information is often off-putting due to the fact that it is difficult to follow or not relevant to them.

The findings emphasised the severe lack of understanding of the basic principles around privacy. As such, the core of the Starter Pack is intended to address two main areas, namely Information Audit and Data Handling, each of which will be implemented in the form of decision trees that the SMEs navigate in order to identify their related data usage and protection needs.

As the Information Audit begins, users are directed through a decision tree to identifying whether their collection of data potentially infringes privacy, before suggesting possible solutions. The audit gives specific consideration to sensitive and personally identifiable information, and considers the need for it to be collected and how it is used. This serves to determines which branches of the Data Handling decision tree are then required by that specific SME. Directing the user to the appropriate branches of the Data Handling tree is where the tool begins to support the implementation of PETs. This approach is similar to the CDEI PETs adoption tool discussed earlier, although addressing an audience with a lower target knowledge level.

At the time of writing the work on the Starter Pack remains a work in progress, and the authors intend to document the outcome and related findings within a future publication.

6 Conclusions

The overall findings from the data collection demonstrate that SMEs generally tend not to think about privacy, or do so at a less extent. For those who do so it is mainly because of risk, potentially after a cyber attack. The main reasons for the lack of attention are lack of necessity and the lack of skills. By highlighting the need for organisations to understand the nature of the risk and the probability of an event occurring, the security approaches highlight the need to address both the threats and actions in the event of an incident to reduce the risk to privacy [33].

In relation to privacy decision-making, the majority of participants indicated that they use internal expert input, and online resources to make such decisions. Our findings also identified several drivers for implementing privacy, including the potential of being fined, reputation damage, the demands of customers, the desire to avoid potential loss, legal or regulatory compliance, and gaining new business. Forcing SMEs to meet best practices (or, in case of supply chains, follow the practices of a lead, and often cyber mature organisation) is not effective. In addition, the language, demands, and expectations are too technical and therefore easily misunderstood and then misapplied.

These findings agree with reseach conducted by [34] showing that the drivers for implementing security and privacy in SMEs are the demands by customers, the perceived threat of losing an important customer, regulatory compliance requirements; and the desire to avoid reputation damage.

Along the lines of promoting an understanding of risks emerging from incidents such as a data breach, the actions necessary to allow SMEs to benefit from and use of PETs is needed. Previous work from the Royal Society [7] sought to explain and scope some of the available PETs alongside their current development and potential through case studies and a sample of some technologies, that are ready for use and others in prototype phases. The application of the technologies chosen in the study either are only relevant to individuals or would require a dedicated expertise within an organisation, or significant outside support.

As shown in previous studies in relation to security [35] skilled personnel, technology readiness, data security concerns, data privacy concerns, legal compliance, and trust in cloud service providers are essential determinants of the intention to adopt cloud computing by SMEs. Our results in relation to privacy showed that to best support the use PETs requirements such as the provision of clear instructions on how personal data may be processed, the provision of clear requirements on obtaining personal data and tools for implementing PETs as well as skilled employees are needed.

Our findings also identified a number of drivers for implementing privacy, mainly the potential for reputation damage, the demands of customers, the desire to avoid potential loss, being part of the 'license to operate' perception, compliance, avoiding the threat of losing a customer and gaining new business. These can be factors that need to be better communicated to SMEs in order to change their perceptions and attitudes around privacy.

On this basis, the findings were taken forward to inform the development of an SME Privacy Starter Pack, which includes pathways for contextualising privacy requirements through scenarios, and real case studies. This aims to provide SMEs with guidance that takes into account the local business environment and cyber threat landscape, raise awareness of the scale of the threat facing these organisations, encourage and incentivise them to invest the time needed to make best use of the available tools such as PETs, and improve their overall privacy posture.

Acknowldgements

References

1. Bada, M., Nurse, J.R.C.: Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information and Computer Security, 27(3), 393-410 (2019), https://doi.org/10.1108/ICS-07-2018-0080

2. European Union Agency for Cybersecurity, ENISA. Cybersecurity for SMEs (2021). https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes, last accessed 2022/7/11.
3. DCMS. Cyber Security Breaches Survey (2022). Department for Digital, Culture, Media and Sport, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022, last accessed 2022/7/11.
4. Sirur, S., Nurse, J. R.C., 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 (MPS '18), pp. 88–95. Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3267357.3267368
5. The Department for Digital, Culture, Media and Sport, Cyber Security Breaches Survey (2022). https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#chapter-5-incidence-and-impact-of-breaches-or-attacks, last accessed 2022/7/11.
6. Cisco. Data Privacy Benchmark Study (2023). https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html, last accessed 2022/7/11.
7. The Royal Society. Protecting privacy in practice: The current use, development, and limits of Privacy Enhancing Technologies in data analysis, 5, (2019).
8. Centre for Data Ethics and Innovation. PETs Adoption Guide. https://cdeiuk.github.io/pets-adoption-guide/adoption-guide/, last accessed 27/09/2022.
9. European Union Agency for Cybersecurity, ENISA. https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies, last accessed 2022/7/11.
10. European Union Agency for Cybersecurity, ENISA. Study on the availability of trustworthy online privacy tools for the general public (2015). https://www.enisa.europa.eu/publications/privacy-tools-for-the-general-public, last accessed 2022/7/11.
11. Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J., Metayer, D. L., Tirtea, R., Schiner, S.: Privacy and data protection by design – from policy to engineering. CoRR, (2015), http://arxiv.org/abs/1501.03726
12. European Union Agency for Cybersecurity, ENISA. PETs controls matrix - A systematic approach for assessing online and mobile privacy tools (2016). https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools, last accessed 2022/7/11.
13. NIST Privacy Framework. https://www.nist.gov/privacy-framework/privacy-framework
14. NIST Special Publication 800-53A1. Assessing Security and Privacy Controls in Information Systems and Organizations (2022). https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final
15. ICO, E-Learning, posters and stickers. https://ico.org.uk/for-organisations/posters-stickers-and-e-learning/, last accessed 27/09/2022.
16. Reset the Net: Privacy Pack. www.resetthenet.org, last accessed 27/09/2022.
17. Best Privacy Tools, bestprivacytools.com, last accessed 27/09/2022.
18. Internet Privacy Tools, privacytools.freeservers.com, last accessed 27/09/2022.
19. Tolsdorf, J., Dehling, F., Iacono, L.L.: Data cart – designing a tool for the GDPR-compliant handling of personal data by employees. Behaviour & Information Technology, 41(10), 2084-2119 (2022). DOI: 10.1080/0144929X.2022.2069596
20. AMBIENT-Automated Cyber and Privacy Risk Management Toolkit, https://www.mdpi.com/1424-8220/21/16/5493, last accessed 27/09/2022.

21. European Union Agency for Cybersecurity, ENISA. A tool on Privacy Enhancing Technologies (PETs) knowledge management and maturity assessment (2018). https://www.enisa.europa.eu/publications/pets-maturity-tool, last accessed 2022/7/11.
22. European Union Agency for Cybersecurity, ENISA. Privacy Enhancing Technologies: Evolution and State of the Art (2017). https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art, last accessed 2022/7/11.
23. European Union Agency for Cybersecurity, ENISA. PETs Maturity Assessment Repository (2017). https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository, last accessed 2022/7/11.
24. ICO. Self assessment checklist. https://ico.org.uk/for-organisations/sme-web-hub/checklists/assessment-for-small-business-owners-and-sole-traders/, last accessed 27/09/2022.
25. GCA Cybersecurity Toolkit for Small Business. https://gcatoolkit.org/smallbusiness/?utm_source=IFA&utm_medium=Website, last accessed 2022/7/11.
26. European Union Agency for Cybersecurity, ENISA (2016). Guidelines for SMEs on the security of personal data processing. https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing, last accessed 2022/7/11.
27. Sangani, N. K., Velmurugan, P., Vithani, T., Madiajagan, M.: Security & Privacy Architecture as a service for Small and Medium Enterprises. In: Proceedings of the *International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)* pp. 16-21. Dubai, United Arab Emirates (2012). doi: 10.1109/ICCCTAM.2012.*6488064.*
28. Corbin, J., Strauss, A.: Grounded theory research: Procedures, canons, and evaluative criteria. Qualitative Sociology.
29. National Research on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN). https://www.rephrain.ac.uk, last accessed 2022/7/11.
30. The Federation of Small Businesses (FSB). https://www.fsb.org.uk, last accessed 2022/7/11.
31. Kratzer, S., Drechsler, A., Westner, M. et al.: The Fractional CIO in SMEs: conceptualization and research agenda. Inf Syst E-Bus Manage, 20, 581–611 (2022). https://doi.org/10.1007/s10257-022-00557-4
32. RISCS, About US. Research Institute for Socio-technical Cyber Security. https://www.riscs.org.uk/about/, last accessed 27/09/2022
33. Allison, I., Strangwick, C.: Privacy through Security: Policy and Practice in a Small-Medium Enterprise. In: Subramanian, R., (eds.) Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions, 157-179 (2008).
34. Lacey, D., James, B.E.: Review of Availability of Advice on Security for Small/Medium Sized Organisations. ICO (2010). https://ico.org.uk/media/about-the-ico/documents/1042344/review-availablility-of-security-advice-for-sme.pdf
35. Nagahawatta, R., Warren, M., Salzman, S., Lokuge, S.: Security and Privacy Factors Influencing the Adoption of Cloud Computing in Australian SMEs. In: *PACIS 2021* Proceedings, p.7. Dubai (2021). https://aisel.aisnet.org/pacis2021/7