# Papers, Peons, and Power: The Challenges of Implementing Privacy Regulations in a Developing Country

Kenneth Thilakarathna
University of Kelaniya
Kelaniya, Sri Lanka

Dilanga Harshani
University of Colombo
School of Computing
Colombo, Sri Lanka

Nathan Malkin
New Jersey Institute of Technology
Newark, NJ, USA

## Abstract

Privacy and data protection regulations are spreading around the world, but our current understanding of the implementation process is shaped primarily by post hoc studies in developed countries. Sri Lanka, a South Asian country with a lower-middle-income economy, recently passed the Personal Data Protection Act, but it has not come into effect yet. This provided us with a unique opportunity to study the pre-enforcement journey of the regulation's implementation. We interviewed 35 stakeholders from organizations of varying scales, including both government and private-sector entities, in roles ranging from C-suite executives to developers. Despite looming deadlines, organizations were only beginning to plan, with significant gaps in understanding and even awareness of the Act. They faced various challenges, some of which echoed those in developed countries, while others were different, such as reliance on non-digital infrastructure, intermediation by informal support staff ("peons"), and weaknesses in enforcement processes. Our findings offer insights into how new privacy regulations can be more effective when implemented in Majority World countries.

## CCS Concepts

• **Security and privacy → Social aspects of security and privacy**.

## Keywords

Privacy Regulations, Data Protection Compliance, Developing Countries, Qualitative Study, Sri Lanka

**ACM Reference Format:**
Kenneth Thilakarathna, Dilanga Harshani, and Nathan Malkin. 2026. Papers, Peons, and Power: The Challenges of Implementing Privacy Regulations in a Developing Country. In *Proceedings of the 2026 ACM SIGSAC Conference on Computer and Communications Security (CCS '26), November 15–19, 2026, The Hague, Netherlands.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3830454.3846771

## 1 Introduction

Privacy regulations are increasingly seen as necessary by societies around the world, driven by increases in the collection of personal data, its value for applications like artificial intelligence, and the market pressures dictating its use [14]. Regulations from Western countries, such as the General Data Protection Regulation (GDPR) [12] and the California Consumer Privacy Act (CCPA) [5], have set the tone for other data protection laws, with many countries following in their footsteps and adopting policies and frameworks, including nations such as Thailand [56], Brazil [35], and Indonesia [18]. While previous work has extensively examined the privacy landscape of the originator countries [1, 7, 8, 11, 16, 25, 26, 39, 43, 48, 50, 52, 54], much of the new privacy legislation is appearing in developing countries, and their experiences remain relatively underexplored. Furthermore, most existing studies examine ecosystems only after the enforcement of regulations [1, 7, 16, 25, 39, 48, 54]; the privacy landscape prior to enforcement, and the process of implementation itself, have not received enough attention.

Sri Lanka, a developing South Asian country with a lower-middle-income economy [62], enacted its Personal Data Protection Act (PDPA) in March 2022 [40]. However, the government has repeatedly postponed the enforcement date of the Act, giving regulated institutions more than four years to prepare for the compliance requirement. This provided us with a unique opportunity to explore the privacy landscape of a developing country before the enforcement of regulations, as well as stakeholders' journeys to comply with them.

Previous studies on privacy regulation compliance in web and mobile applications in Sri Lanka have revealed that compliance rates are very low even after more than two years since PDPA was enacted [45, 57], suggesting little progress in the privacy ecosystem. This observation raises an important question: why are stakeholders not actively working toward compliance? It is imperative to understand the underlying causes and identify existing issues in order to create a better privacy ecosystem in Sri Lanka. The country's experiences can furthermore guide improvements in the rollout of privacy legislation for countries that are still considering their own.

To address this gap, we developed a set of research questions aimed at better understanding the pre-implementation phase and the costs and challenges implementers encounter during it, especially those arising due to fundamental factors like culture:

(1) How do organizations plan for upcoming regulations, and what is the current state of their preparations?
(2) What is the role of the regulator in helping organizations?
(3) What role do cultural norms play?
(4) What technical challenges do stakeholders encounter?
(5) How do stakeholders perceive the cost and budget of implementation?

We conducted 35 semi-structured interviews with management and technical professionals from government and private-sector organizations of different scales. Our findings shed light on the state of privacy compliance at a time when stakeholders had almost four

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
*CCS '26, The Hague, Netherlands*
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2871-6/2026/11
https://doi.org/10.1145/3830454.3846771

PREPRINT

years to comply with the PDPA. They reveal that most government and private-sector organizations are at the very beginning of the planning stage. Few organizations had progressed in their implementation to adhere to the PDPA, and those that had were mostly from the financial sector. Furthermore, we identified a significant gap in awareness of the Act, as well as a lack of sufficient guidance from the regulator regarding implementation. Our findings also revealed that stakeholders encountered various technical, cultural, and financial challenges. Additionally, many participants did not see direct benefits of compliance other than avoiding penalties, largely due to a lack of perceived consumer demand. They also lacked trust in the government's ability to fully enforce the Act.

## 2 Background and related work

### 2.1 Sri Lanka's PDPA

The majority of the world's countries have passed some form of privacy law [14]; one of them is Sri Lanka. The Democratic Socialist Republic of Sri Lanka is a developing South Asian, lower-middle-income country with a presidential system [62]. According to a 2024 census, Sri Lanka has a population of approximately 21.7 million, with its capital Colombo being the most densely populated city and holding more than 11% of the population [10].

Sri Lanka enacted its first privacy act, the Personal Data Protection Act (PDPA), in March 2022 [40]. The initial enforcement date was set for March 2025, creating a three-year timeline for compliance. Subsequently, however, the enforcement deadline was extended by six months, and then extended again, this time indefinitely, through an October 2025 amendment [41].

Unlike many other privacy regulations, the Act applies to both private sector *and* government bodies.[1] Under the Act, data controllers must adhere to core data protection obligations identical to those in the GDPR, such as lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. Like the GDPR, the Act identifies and strengthens key rights for individuals: right to be informed, right of access, right to withdraw consent, right to object, right to rectification, right to erasure, right to restriction, right to data portability, and right to request a review of decisions based solely on automated processing that significantly impacts them. While PDPA is modeled on the GDPR, the law is less detailed and has a few other differences [12, 40].[2]

Another aspect of the Act was establishing the Data Protection Authority of Sri Lanka as an agency to regulate processing and ensure compliance. Its authority includes conducting inquiries, receiving complaints, inspecting premises, and issuing binding directives to controllers and processors. Originally, all entities under the purview of PDPA needed to have a Data Protection Officer (DPO) to oversee compliance. However, the 2025 amendment dispensed with the mandatory requirement for public corporations, which are considered government entities [42], to appoint a DPO. Further, the DPO no longer has the responsibility of ensuring an entity's compliance, making the role purely advisory [41, Section 20].

Despite the PDPA being enacted for more than two years, an empirical study of Sri Lankan health sector mobile applications and websites conducted in 2024 revealed very low compliance rates [57]. Another study on privacy regulations and compliance in Sri Lankan web applications found similar results, further confirming this situation [45]. It is worth noting, however, that similar compliance delays have been observed with other regulations. Organizations continue to violate privacy regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) years after their enforcement, and several studies have identified interpreting legal documents, regulatory support, culture, awareness, and cost as key challenges driving this non-compliance [13, 27, 38].

### 2.2 Interpreting regulations and regulator support

Several studies using semi-structured interviews revealed that stakeholders involved in implementing GDPR compliance face significant challenges. After interviewing privacy compliance implementers and surveying developers, researchers identified that understanding legal requirements and translating them into technical solutions is a major challenge for implementers [11, 49]. However, some stakeholders believe that privacy laws and regulations remain unclear until cases are prosecuted and interpreted, demotivating implementation efforts [50]. Interviews with software development teams and a comparative study of data protection regulations have pointed out that a lack of clear guidance on using specific technologies also affects implementations [24, 54, 63]. Furthermore, interviews with privacy implementers revealed that they did not receive sufficient support from regulatory authorities to overcome implementation challenges [39, 50]. All these factors add complexity to implementing privacy features in digital systems [11, 24, 32, 39, 49, 54, 63]. Consequently, studies highlight that implementers need early support to avoid legal problems later in the compliance process [48]. Furthermore, implementers emphasize the need for a proper system to identify competent privacy domain experts and a verification mechanism to evaluate their compliance state at a given stage of implementation [26, 49, 54]. On the other hand, interviews with privacy experts and examination of government budgets suggest that governments themselves occasionally lack the resources to adequately fund data protection authorities for enforcement [7].

### 2.3 Privacy culture

Through interviewing developers and C-suite executives across various organizations, researchers have identified that both employees' personal privacy perceptions and organizational norms affect privacy implementations, and changing such culture is a non-trivial task [2, 49, 52, 61]. In building a privacy culture, some research recognizes strategies such as introducing a specialist role called a "privacy champion," a person with privacy training and awareness, to gradually shift the organization towards a privacy culture [54]. However, interviews with technical privacy experts revealed that organizations often do not consider privacy a core value [16], nor do they provide enough time and autonomy to build

[1] The Act specifically names the following covered public and private entities: those who process personal data of those wholly or partly within Sri Lanka; by a controller or processor domiciled, ordinarily resident, or incorporated in Sri Lanka; by entities that offer goods or services to data subjects in Sri Lanka; and by entities that monitor the behavior of data subjects within Sri Lanka.

[2] Unlike in the GDPR, the role and independence of an organization's Data Protection Officer is not explicitly defined under PDPA. Additionally, the GDPR has two penalty tiers, depending on the severity of violations, with fines defined as a percentage of global annual turnover, while PDPA penalties are capped at 10 million LKR.

PREPRINT

ethical systems [52]. Exacerbating the situation, interviews with software developers revealed that the organizational climate sometimes allows, and even promotes, behaviors against privacy [17].

## 2.4 Privacy awareness

Several studies identify a lack of awareness regarding privacy regulations, benefits, and consequences as a factor driving prevailing compliance issues. Interviews also revealed that organizations do not see a competitive advantage in being compliant and lack the required capacity, thus failing to prioritize compliance implementation [54]. Findings from the literature indicate that organizations tend to prioritize privacy and security only as their business and products mature [8, 50]. Interestingly, Hadar et al. found through interviews with developers that many confuse security with privacy, making achieving compliance more difficult during product development [17].

## 2.5 Solution implementation challenges

A literature review conducted by Zaguir et al. identified that stakeholders see challenges in adhering to the right to revoke consent and the right to be forgotten when products integrate emerging technologies like big data analytics and artificial intelligence, as they facilitate the re-identification of personal data. Consequently, organizations fear that regulatory restrictions may decrease their performance, product offerings, and ability to scale internationally [48, 63]. Additionally, Ekman and Billgren found that making legacy systems compliant with the GDPR was difficult because stakeholders found it economically infeasible to understand the technological landscape, learn where data resides, make data processes compliant, and redesign all systems to adhere to the law [11]. According to Poritskiy et al. and Li et al., smaller organizations are hesitant to modify existing systems due to the increased technical complexity introduced by compliance [26, 43]. Additionally, several studies reveal that participants view compliance as an increase in administrative and operational work [43, 48, 63], while Chen et al. found, through semi-structured interviews of entrepreneurs, that they find user data to be a profitable asset, and investor pressure for profits leads them to deprioritize privacy and security [8].

## 2.6 Cost of compliance

Expertise, time, resources, changes to processes, and operations incur costs. Zaguir et al. show that organizations lack expertise in privacy and need to recruit specialists [63]. Recruiting and retaining specialist professionals such as a DPO is difficult [63]. Even if specialized resources are available, studies highlight that teaming up experts from different disciplines, such as developers and lawyers, has not produced the intended results due to interdisciplinary communication issues or, in some cases, a complete lack of communication [25, 54]. Handling the resulting legal issues also increases costs and resource requirements [11, 48]. Maintaining compliance requires security operations and regular audits, which add to the overall cost [43]. Research shows that organizations find GDPR compliance expensive and struggle to allocate required budgets, suggesting that developing countries should design their laws and enforcement structures with compliance costs in mind [7, 63].

## 2.7 Studies on privacy challenges in South and Southeast Asia

Most studies on privacy implementation and its challenges are post-enforcement studies focusing on developed countries. The situation faced by South Asian countries could be different. A limited number of studies has been carried out in the South Asian region relating to privacy implementations [20–22, 44, 46, 47, 55]. Of these, only one study, by Prasetyo et al., used in-depth interviews and focus group discussions with Indonesian stakeholders to identify challenges in implementing compliance [44]. It identified prominent challenges including low public awareness, stakeholder resistance due to business models, regulatory bodies lacking resources to enforce policies, political and economic interference, and small and medium-sized enterprises viewing compliance as a burden. However, the study lacks population information, making it difficult to clearly contextualize the outcomes.

Sri Lanka is the first country to enact a comprehensive, standalone data protection act in South Asia [9]. As South Asian countries show increasing interest in privacy regulations, we see a significant gap in studying implementation challenges with stakeholders prior to enforcement. Sri Lanka is a lower-middle-income country where the majority of the population struggles with economic and financial stability, a factor not present in the wealthy nations that dominate the privacy regulation literature [62]. Exacerbating the financial difficulties is the fact that Sri Lanka went through a sovereign debt default, declared on April 12, 2022, just after the PDPA's enactment [31]. Additionally, the country's corruption levels affect many industries, reflecting the nature of policy and law enforcement [59]; studying how stakeholders approach a privacy law in this environment is crucial for understanding future implementations in similar regions.

Our study contributes to the global discourse on privacy regulations by providing empirical evidence of implementation challenges in a country categorized by the International Monetary Fund (IMF) under Emerging Market and Developing Economies (EMDEs) [3, 19]. By documenting the findings during the pre-enforcement phase in a lower-middle-income context, our study surfaces issues that may affect the more than 50 other nations under the category of EMDE, including regional peers like Bangladesh and Pakistan, who are currently navigating similar transitions [15, 60].

# 3 Methods

Between May and November 2025, we conducted 35 semi-structured interviews with senior managers, middle managers, and developers at private organizations and government entities that are directly subject to the PDPA either as data controllers or as processors.

## 3.1 Research design

We developed the protocol for our semi-structured interviews based on a literature review of global data protection compliance and privacy regulation implementations. The protocol focused on five main topics we wanted to explore:

(1) *Compliance requirements and resources.* Prior literature establishes that clear requirements and resource availability are critical for compliance [11, 16, 25, 28]. We therefore designed questions to elicit stakeholders' insights on these

PREPRINT

factors in the local context, such as how implementers interpret the PDPA's requirements and where they find the resources needed for compliance.

(2) *Regulator's role.* Stakeholders' expectations regarding regulator support and guidance can indicate gaps in the enforcement process. Furthermore, these expectations provide insights into the regulator's involvement during the pre-enforcement period.

(3) *Culture.* Sri Lanka has a highly open culture regarding social interactions and communication, contrasting with the U.S. and European countries where most privacy compliance studies have been conducted [58]. Thus, we sought to understand how these cultural norms affect compliance implementation.

(4) *Challenges.* Understanding the challenges stakeholders face during implementation is a core objective of our study. Therefore, we asked broad, open-ended questions to identify perceived challenges and potential solutions from the stakeholders' perspectives.

(5) *Cost of compliance.* Sri Lanka is a developing country that faced a severe financial crisis in early 2022, the same year the PDPA was enacted [62]. Even small and medium-sized enterprises (SMEs) in developed countries find compliance costs burdensome [32, 50, 51]. Therefore, organizations' financial perceptions of compliance efforts are likely a crucial factor in their motivation to adhere to the PDPA.

After drafting the protocol, we refined it using feedback from domain experts and conducted pilot interviews to improve the instrument's clarity and effectiveness.

## 3.2 Participant recruitment

We recruited interview participants using a stratified snowball sampling approach, choosing this method because initial interactions revealed that stakeholders were reluctant to discuss their compliance posture with strangers. We screened job titles and role descriptions for decision-making or implementation responsibilities related to security/privacy, compliance, or PDPA. We aimed to achieve diversity across government and private sectors, as well as across hierarchical and professional roles. This need to reach specific job-level strata further motivated our sampling choice. Informed by the literature, we defined senior managers, middle managers, and developers as our target strata. We identified and contacted initial participants through professional and academic networks. We then asked them to recommend other suitable participants.

In total, we conducted 37 interviews, nine through direct contact and the rest using snowballing. Two were pilot participants who met the selection criteria and whose sessions were used to refine the flow and interview questions. Of the remaining 35 participants, 14 represented government institutions and 21 represented private-sector organizations. The former included some organizations that handled data applicable to every Sri Lankan; the latter ranged in size from small startups to large corporations with more than 200 employees. As Table 1 shows, these organizations span domains such as finance, software development, and services like health, education, telecommunications, and transport. Our sample included a wide range of roles, from senior executives (CTOs, CIOs, CEOs, and directors) to middle managers responsible for handling data protection compliance. The 35 participants represented 30 distinct organizations; repetitions arise from cases when we interviewed developers and engineers from the same organizations to obtain a holistic perspective on their practices. We continued data collection until each new interview was found to yield limited new insights.

**Table 1: Organization details of interview participants**

| ID | Type | Domain | Designation |
|---|---|---|---|
| P01 | Govt. | Services | Middle Mgmt, Developer |
| P02 | Govt. | Finance | Middle Management |
| P03 | Govt. | Finance, Software | Developer |
| P04 | Govt. | Services | Middle Management |
| P05 | Govt. | Finance | Middle Mgmt, Developer |
| P06 | Govt. | Services | Senior Management |
| P07 | Govt. | Services | Middle Management |
| P08 | Govt. | Services | Senior Management |
| P09 | Govt. | Finance | Middle Management |
| P10 | Govt. | Finance | Senior Management |
| P11 | Govt. | Services | Senior Management |
| P12 | Govt. | Services, Software | Senior Management |
| P13 | Govt. | Services | Middle Management |
| P14 | Govt. | Services | Middle Management |
| P15 | Large | Finance | Senior Management |
| P16 | Large | Finance | Senior Management |
| P17 | Large | Services, Software | Senior Management |
| P18 | Large | Services, Software | Middle Management |
| P19 | Large | Services, Software | Senior Management |
| P20 | Large | Services, Software | Developer |
| P21 | Large | Finance | Senior Management |
| P22 | Large | Services, Software | Senior Management |
| P23 | Large | Services, Software | Developer |
| P24 | Small | Services | Developer |
| P25 | Medium | Services, Software | Senior Management |
| P26 | Small | Services, Software | Senior Management |
| P27 | Small | Services | Senior Management |
| P28 | Small | Services, Software | Senior Management |
| P29 | Small | Services, Software | Developer |
| P30 | Startup | Services, Software | Senior Management |
| P31 | Startup | Finance, Software | Senior Management |
| P32 | Startup | Software | Senior Management |
| P33 | Startup | Software | Senior Management |
| P34 | Startup | Software | Senior Management |
| P35 | Startup | Software | Senior Management |

Govt. — Government, Large — Large Enterprises with ≥ 200 Employees, Medium — Medium Enterprises with 50–200 Employees, Small — Small Enterprises with < 50 Employees

## 3.3 Data collection

We conducted interviews in person and through video conferencing, depending on participant preference. Each session lasted approximately 30 to 45 minutes. While a fixed protocol guided the interviews, we adjusted the order and emphasis of questions based on the conversation's flow. Interviews were conducted primarily in

PREPRINT

English, with occasional exchanges in Sinhala (the most common native language in Sri Lanka) based on participant preference. Two researchers were present for each interview, with one leading the interview and the other taking detailed manual notes (in English) documenting participants' responses. We used this approach in lieu of recording audio or video in order to protect participant confidentiality and strengthen their confidence in providing candid opinions.

### 3.4 Data analysis

We organized and transcribed our interview notes immediately after each session to ensure accuracy and completeness. We removed all identifying details from the transcripts to preserve anonymity and stored them securely with restricted access. We used thematic analysis to identify patterns in the data, following Braun and Clarke's [4] six-phase framework: familiarization, initial coding, searching for themes, reviewing themes, defining themes, and producing the final analysis. Our coding process was inductive, allowing themes to emerge from the data rather than relying on predefined categories. Two researchers coded the data independently, discussing and resolving discrepancies promptly to ensure analytical consistency. Both coders conducted all interviews together, providing preliminary familiarity and insight into the material. The coders independently went through three transcripts multiple times and iterated on codes before discussing and merging them into the initial codebook. After each subsequent interview, they met to discuss and jointly update the codebook as necessary. No new themes appeared for the research questions in the last 3–5 interviews for both government and private organizations (and answers became predictable even during the interview itself), at which point we ended recruitment. Due to the nature of our process, we did not calculate inter-rater reliability metrics [29]. We used spreadsheet applications with automated scripting to manage the collaborative analysis and maintain an auditable record of the process.

### 3.5 Ethics and positionality

We obtained ethical clearance from our affiliated institution and collected informed consent from every participant, as detailed in Appendix B. The lead researchers who conducted the interviews, processed the data, and performed the thematic analysis are Sri Lankan citizens with computer science backgrounds, providing them with familiarity with the local context and culture.

### 3.6 Limitations

Our study has limitations common to qualitative research. The thematic analysis procedure is inherently subjective to the researchers' interpretations. Our findings are based on the interviewees' opinions and experiences and cannot be generalized more broadly (e.g., to all PDPA implementers) or considered as representative. For this reason, we also refrain from reporting quantitative measures and tendencies. While we hope the study's findings are applicable to other countries or cultures, we cannot draw such conclusions on the basis of our data alone. Our sampling provided representation of many sectors and domains but is not uniformly distributed. Similarly, most of the participants were located in Colombo, the capital of Sri Lanka, which is the most populated, digitized, and commercial area in the country. The sample is further biased by recruitment that relied on our professional networks and snowball sampling. While we made clear to our participants that their responses would be anonymized, they may have still been reluctant to share certain information due to lack of trust or because of organizational obligations. Finally, our interviews focus on the perspectives of organizations implementing PDPA and their staff; we did not interview the other side—the regulators—who may hold differing views and complementary insights.

## 4 Findings

Our interviews reveal the challenges of navigating a diversified privacy landscape during the implementation of the PDPA. We organize the findings into five primary themes: (1) stakeholder preparedness for enforcement; (2) understanding of the Act and the regulator's role; (3) organizational and public privacy culture; (4) technical challenges; and (5) perceptions of compliance costs.

### 4.1 Stakeholder preparedness for PDPA compliance

In regulatory enforcement, it is standard practice to allow stakeholders a grace period to align their personnel, processes, and technologies with new requirements. The PDPA provided a three-year window for these preparations. Our first research question explores how organizations plan to prepare for these regulations and the current state of their readiness.

*4.1.1 Stakeholders show slow progress in implementation with limited confidence or direction.* Participants reported being at the early stages of implementation, often lacking a clear roadmap or the confidence to proceed. Current activities primarily involve conducting awareness programs, performing gap analyses, developing policies, or implementing information security controls. Efforts are largely focused on information security, digitization, and automation. In-house software development and security teams are perceived as significant advantages, providing organizations with higher confidence in their technical implementation. Some participants believe a security team alone is sufficient for compliance, such as P30, who said, *"we have an information security function for internal system control and deployment requirements … so implementation expertise is there."*

Participants from organizations with prior compliance experience (e.g., PCI-DSS or ISO 27001) or those serving international clients (requiring compliance with GDPR or Australia's OAIC) described more mature plans with clear next steps. Large corporations expressed the most confidence, citing financial resources, management support, and existing audit infrastructure. One large corporation senior manager, P21, highlighted their internal expertise: *"We are in a bit of a unique situation. We have a veteran in this field in our board who is a pioneer in this data protection and privacy area."* These participants shared practical insights, such as prioritizing data classification followed by implementing controls for collection, retention, and sharing.

Conversely, participants outside the financial sector expressed less confidence in their ability to comply. Notably, none of the participants described plans for handling data subject rights, such as requests for erasure or withdrawal of consent. Furthermore, most

PREPRINT

participants did not address the Act's limitations on cross-border data transfers. Several participants, particularly in the government and startup sectors, lacked a formal compliance plan. Some perceived themselves as low-risk targets; for instance, P07 remarked, *"what can hackers get from us? There is nothing to take from us so who is going to hack us?"*

*4.1.2 Motivation for compliance is driven by reputation, liability, and regulatory mandates.* For most organizations in the early or middle stages of implementation, the primary motivation for compliance is avoiding reputational damage or legal penalties. For the financial sector, however, compliance is mandatory and driven by the Central Bank of Sri Lanka (CBSL) [6], the nation's financial regulator.

Beyond legal requirements, some participants view compliance as an opportunity to transition from ad-hoc processes (e.g., multiple software tools used by different people for similar tasks) to standardized software practices and formalized data management. Others view it as their responsibility to comply.

Interestingly, some government participants saw the PDPA as a lever to reclaim data ownership from third-party software vendors. P09, from a government organization in finance, explained: *"When we request access to these data they were telling us that they can't give access because these are sensitive data. They have forgotten who the data owner is. We are having discussions on this with them, highlighting this PDPA Act, before we had nothing to bring this up."* Many participants suggested that enforcement should rely on audits, with several advocating for strict penalties meant to induce fear.

*4.1.3 Stakeholders seek expertise to interpret the Act and map requirements.* Organizations recognized the need for specialized expertise to interpret the Act and map its requirements to technical controls, yet they faced significant hiring constraints. Most interviewees described wanting a lawyer with information technology knowledge to understand the Act, like P25, who said, *"what we need is to look at this from the legal side with regards to the Act and government laws."* Finding such experts is challenging; P15 expressed that it is *"very difficult to find expertise in Sri Lanka [where the talent pool is] not very mature."*

Uncertainty regarding enforcement and long-term operational costs led many to prefer external consultants over permanent hires, with P26, a senior manager from an SME, stating they are *"not planning to take permanent resources, hence expect consultation."*

Government organizations faced additional barriers like strict procurement processes, a lack of allocated staff positions for privacy roles, and no budgets. Even the recruitment process itself presents pitfalls; P04, for example, noted that *"we don't have [. . . ] positions or a procedure to recruit people for this."* In the face of this, some participants proceeded using existing internal staff, relying on their own interpretations of the Act rather than seeking specialized guidance.

## 4.2 Understanding the Act and regulator's role

When a new privacy act is adopted, stakeholders need to understand its requirements and expectations—a process in which the regulatory authority typically plays an important role. Our second research question aimed to understand the stakeholders' experiences and expectations for the regulator's role. Our findings reveal that most participants find it difficult to interpret the Act; furthermore, nearly all participants expressed dissatisfaction with the guidance provided by the government and the Data Protection Authority (DPA).

*4.2.1 Understanding and interpreting the Act.* Most participants found the Act difficult to interpret for implementation; for example, P05 opined that *"technical people cannot understand pure legal interpretations, therefore that legal to tech map should be there. DPA should do awareness programs combining them."* Participants often believed that a lawyer with information technology expertise would be necessary to bridge this gap. Furthermore, they look to the DPA to provide the necessary support for understanding the legislation. They also suggested that the DPA should provide guidelines featuring a phased approach and checklists detailing how specific controls map to clauses in the Act. *"it would be good if they can give sector specific guidelines. . . that would be easier for everyone"* (P17). A few suggested a need for specific guidelines tailored to different professional roles, such as management, architects, and developers.

A majority of participants reported that they had not yet appointed a Data Protection Officer (DPO), despite this being a PDPA requirement. Participants emphasized that the Act does not clearly define the DPO's roles and responsibilities, hindering the recruitment process; for instance, P09 said *"Even though it says to appoint a DPO, we have no idea what that person should do and what are their duties."* However, most large corporations have already recruited a DPO, sometimes planning to assign the role to existing employees, such as risk and compliance managers.

*4.2.2 Stakeholders learn about compliance requirements incidentally rather than from regulator.* Successful compliance depends on awareness and understanding by covered entities, but our interviews revealed significant gaps in awareness and communication more than two years after the PDPA's enactment. Some participants were entirely unaware of the PDPA. Among the majority who were aware, many learned of the Act incidentally—through potential clients or professional networks (e.g., posts on LinkedIn and other social media)—highlighting a significant communication gap. Several participants incorrectly assumed the responsible entity was the Computer Emergency Readiness Team of Sri Lanka (SL-CERT). They were surprised to learn of the existence of the Data Protection Authority (DPA), such as P27, who *"did not know there is an authority like that even."* In contrast, participants from the financial sector had been made aware of the PDPA by the CBSL. However, even those who were aware of the Act called out its ambiguities, such as P19, who noted that *"there are certain ambiguity areas like how it works with data sharing among groups of companies."*

*4.2.3 Stakeholders say the support and guidance from DPA is minimal to none.* All interviewed participants stated that the DPA has provided insufficient awareness, guidelines, and support for both implementers and the general public. Due to the lack of local resources, some participants have instead turned to GDPR guidelines; P19 explained: *"we do not get much insight from them (DPA), that is why we are independently relying on our consultants and relating our problems to GDPR. That is easier than getting from DPA."* Participants highlighted the challenges of lacking domain-specific guidelines, tutorials, training materials, or checklists. P13 said, *"in DPA discussions they state that they are going to do this and that,*

PREPRINT

*but when it comes to the ground level there is nothing. There is no answer when we request some recommendation even. We need a way to verify what we are doing."*

Some participants raised concerns regarding weaknesses of the prevailing legal and governance systems, citing unreliable government decisions, loopholes in the legal system that could be used to avoid penalties, potential business losses due to systemic delays, and a lack of oversight through auditing or monitoring. For example, P26 expressed their skepticism, noting that even if *"the government says they are going to enforce," "in SL, companies know they still can go around and get business done without this."* According to participants, even the legal system did not seem prepared to handle the regulations. For example, P16 pointed out that there was *"no clarification on how to handle PDPA related cases in a court. You have to educate judges and legal people as well."* Furthermore, some participants questioned whether the DPA possesses the necessary expertise; P13 related having *"asked questions at the only workshop we had under the Ministry of [redacted] but did not get any answer, it seems they haven't taken a decision on cloud data storage."* The absence of a functional communication channel for clarifications was also a common concern. Additionally, some participants expressed uncertainty about how the PDPA interacts with other legislation: *"our Act might be superseding the PDPA as we collect a lot of sensitive data and we cannot allow users the right to erase as well"* (P11).

Collectively, the DPA's lack of preparedness has led stakeholders to question the Act's eventual enforcement, its necessity, and the feasibility of aligning business operations and technologies with its requirements.

## 4.3 Privacy culture in organizations and public

Culture influences how people perceive the idea of privacy and its importance. Our next research question focused on understanding the role of cultural norms in implementing new privacy regulations.

*4.3.1 National culture of openness.* Sri Lanka is one of the world's countries where individuals are accustomed to a communal culture, and prior research has found that privacy concerns translate less directly into privacy-protective behavior among Sri Lankans compared to Western populations, indicating a cultural pattern of greater tolerance for information exposure in social and civic contexts [58]. A number of participants brought this up as a barrier to enacting stricter privacy controls, such as P30, who explained, *"culturally we are more inclined to trust and we open up. Sometimes you can't escape a conversation without being rude. This culture doesn't go well with privacy."* P21 elaborated: *"Compared to the Western culture where people are very concerned about privacy, we are in a more open and connected culture so people are not just bothered about sharing personal data."* To overcome this challenge, participants emphasized that individual organizations would need to change their culture first, and that management must play a prominent role in driving these changes.

*4.3.2 Building a privacy-aware organizational culture.* Most participants whose organizations were still in the planning stage of compliance were confident that a cultural shift is not difficult if properly administered, particularly among the IT workforce. Some expressed that, although they anticipated initial resistance, employees will adapt over time.

However, participants from organizations in the middle of compliance implementation held a different view, seeing the cultural and attitudinal change of employees as quite challenging. For example, P17 said, *"we have designed a framework for data governance... We are trying to implement procedures but mostly data gets shared on trust among these people."* These participants suggested that awareness programs should cover data-handling fundamentals, threats and risks, best practices, and ethics. They emphasized that organizations should tailor awareness programs to the employee's role—from management to clerical staff—and cover the privacy aspects of the specific processes in which each person is involved.

Participants from government organizations highlighted that IT staff turnover negatively impacts the compliance process: *"Most people just serve for a limited period and leave so no maintenance or knowledge transfer. As they do not hand over the responsibilities and knowledge properly, no one else will try to learn and maintain them"* (P04, a middle manager from a government organization). Furthermore, most of these organizations find it difficult to convince senior non-IT staff of the importance of compliance. P09 stated that *"government workers, especially non-IT people, are reluctant to embrace updates, they just prefer to stay with the same day-to-day processes."* In this participant's view, senior employees are often unwilling to risk engaging in new initiatives that might affect their retirement plans and government-provided pensions, given the short time left in their careers.

In contrast, most small and medium enterprises (SMEs) and startup organizations focus primarily on expanding their business and increasing revenue, treating compliance as an afterthought. For example, P35 said, *"our main target is revenue and [we are] tight on the resources at the moment."*

*4.3.3 Lack of awareness, facilitation, and direction by management.* Management awareness of the PDPA in the government sector proved to be very low compared with the private and financial sectors. Participants in the middle of the implementation process stated that management awareness is essential for successful compliance, as managers are the primary decision-makers. For example, P15 believed that *"awareness has to be created with some kind of push and it should come from top to bottom."* However, most participants from government organizations reiterated that their management lacks awareness regarding both the importance of compliance and the consequences of non-compliance. One participant, P05, noted that *"awareness should be given to the top positions first because even if we have knowledge we can't execute things without them approving."* As a result, management lacks the required motivation to prioritize compliance implementation. Interestingly, the management of some government organizations has not even communicated compliance requirements to middle management, leading to significant delays in some instances. For example, P05 said *"as the top management lacks awareness on the importance of this, the act they have received is not even properly directed to relevant divisions."* Additionally, several participants reported that bureaucracy negatively impacts implementation. Because managers often come from domains other than information technology and finance, they struggle to understand the importance of privacy compliance. In the words of P05, *"the*

PREPRINT

*first [challenge] thing is the bureaucracy. We are in IT but decisions are taken from the services divisions. In this hierarchy, all top level people don't have an idea on IT related things so it's hard to convince them."*

*4.3.4 Insufficient user awareness of their privacy rights.* Most participants noted that giving users—as actual owners of the data—a good understanding of privacy is pivotal to successful compliance: if customers do not understand privacy and their rights, the privacy ecosystem will not be sustainable. These participants further emphasized that organizations must incorporate new methods to build a privacy-conscious culture among the public in Sri Lanka. P15 gave an example, stating that *"ethical considerations of data should be emphasized. For example, there is no need to ask for your gender or religion when doing a transaction."* Almost all participants felt that the DPA should be responsible for public awareness. However, a few interviewees argued that organizations should also become involved in making the public aware of their privacy rights, building customer trust through employee accountability.

## 4.4 Technical challenges faced by stakeholders during compliance implementation

Adapting to a new practice brings various technical challenges to stakeholders with respect to their day-to-day operations. Our fourth research question focused on understanding these technical challenges. Participants found compliance implementation challenging on prevailing systems and infrastructure, underscoring that the changes would sometimes require re-engineering entire systems and processes. They further raised concerns about the challenges they would face in continuing business operations centered around the use of PII.

*4.4.1 Fulfilling business requirements under the restrictions of compliance.* Participants emphasized that compliance must not be a showstopper for businesses. Harmonizing business needs with privacy compliance was seen as a challenge by some participants, such as P19, who stated, *"When it comes to doing business, we should know where to draw the line of satisfying the authority and doing business as well,"* and noted they were still trying to figure out a solution. On the other hand, others considered privacy compliance an opportunity to win customer trust. Still, some also viewed it as a double-edged sword, where a single data breach could collapse the customer trust gained over many years.

The biggest challenge faced by participants from private-sector organizations was that their products rely on PII or related data from users, such as contact details, user behavior data, and location data. They use this data to maintain the quality of service, improve user experience, and promote products through cross-selling and up-selling. They expressed concern that compliance would entail limitations on collecting such data, and they stated that it would affect users in the future. A few participants had concerns regarding cross-border communication and regulatory compliance, while others were concerned about storing PII on cloud infrastructure.

Participants from government organizations had a different experience with respect to providing services throughout the country due to diverse infrastructure and societal contexts. For example, P08 said, *"Data connection at remote areas is not strong. So officers sometimes share passwords with others with data connection to somehow enter data into the system."* In some circumstances, employees use their personal devices and might also have to put data into the system on behalf of the end user due to a lack of language or technological literacy. For example, P11 stated, *"We have tried giving user guide videos, but the literacy and status of people vary a lot, so it is hard to approach all users."*

*4.4.2 Protecting information in physical documents.* Not all government services are handled through digital systems; physical documents are still sometimes in use. Some participants said that protecting such long-standing, unclassified documents from leakage through employees, auditors, or improper disposal was very difficult. P17 explained: *"Some people still prefer hard-copy form filling. Then we have to be careful [about] how those are discarded after adding data to the systems."* Paper documents may even be a requirement, especially in government processes: *"When it comes to government auditors they need everything in paper, even soft copies we should print and give them as hard copies. How can we do this with systems? Also giving them all our data in hard copies is a method of data leakage too"* (P09).

As another example, documents are often transferred internally within an organization by an aide, called a "peon," who physically carries documents from one government employee to another. (The role may have different names, such as a "works aide," and be performed by workers with other responsibilities, such as a security guard.) This often happens irrespective of the document's sensitivity or criticality, in both government and private organizations. During the transfer process, the person can easily make a copy of the document. Therefore, participants emphasized the need for regulators to provide guidelines on protecting physical documents.

*4.4.3 Developers having limitless access to PII.* Most participants from government organizations said that they have their software developed by third-party software development organizations, and that the developers do not follow standard software practices. Due to a lack of awareness among government officers, these developers often have direct access to user data. In light of this, participants questioned the trustworthiness of developers and raised further issues, such as data ownership and lack of support. Some organizations in the private sector had a similar issue with their own development teams, as they did not have enough resources. For example, P29 said, *"We can't give laptops to all developers, they are using their own laptops so we can't restrict software installations, tools and stuff as well."* However, most participants from the private sector stated that they have internal development teams to build their solutions or have proper access controls when working with third parties.

*4.4.4 Changing current processes and unmanaged software systems.* Many participants said that they needed to re-engineer existing processes for data collection, data access, and data dissemination to align with PDPA compliance. For example, P01 said, *"Our processes will have to be redefined to align with the requirements of the PDPA."* In their case, the process disseminates PII without any consent or control, and there is no way to track what happens to the information after it has been shared. Moreover, as part of this process, PII is read aloud for verification, causing the information to be leaked to

PREPRINT

others in the vicinity, including individuals unknown to the person whose data is being shared. Despite being clearly problematic for privacy, changing such processes may encounter resistance, as one use case for PII is in political campaigns to gain governing power.

The changes required for re-engineering systems differ on a case-by-case basis. Most participants from government organizations said that the use of legacy systems had made integration difficult, and in some cases, had become a blocker for the entire compliance process, requiring development from scratch. Failure to maintain documentation and system details, data management, ownership, and infrastructure was identified as a common weakness in almost all government organizations. Some participants further added that having different versions or entirely different applications across multiple regions, or even within the same department for similar services with duplicate data, was a difficult problem to solve. For example, P14 said, *"Mostly of our systems are like making ad hoc systems whenever something is needed. Branches are using multiple systems."* Not having access to the source code of most systems worsened the situation further. P06, a senior manager from a government organization, said, *"We do not know the infrastructure of the places that our services are hosted. . . . In some of our systems we do not have any documentation so we have no idea how this data is handled over the processes and also how already stored data are stored and steps of the process."*

Participants from private and finance organizations had different issues; for example, P17 wondered how to harmonize a user's right to be forgotten with other legal obligations: *"We have a lot of sensitive information about users. . . [The organization's] governing body says we should keep data for five years, but if the user requests to erase data before that?"* However, most participants did not raise concerns about the user's right to be forgotten, as they had not encountered the finer details of the Act yet.

## 4.5 Perceptions of compliance costs and budgets

Cost and budgetary concerns are important factors when adopting new practices in an organization. Through our fifth research question, we explored how stakeholders perceive the cost and budget of PDPA implementation. Findings reveal that most participants consider compliance a cost due to the lack of demand from clients or users, and some organizations lack an allocated budget.

*4.5.1 Stakeholders see PDPA compliance as a cost with no direct benefits.* Most participants do not consider the cost of compliance an investment, as they see no direct benefit to their business in Sri Lanka's current privacy ecosystem. For example, P30 said, *"When customers start demanding this and asking for this, then it becomes an investment. Until then it will be just a cost without an advantage. It has to become a necessity, not a burden."* Participants from most private organizations believe the limitations imposed by compliance will hinder market insights, negatively impacting business. Therefore, most participants from SMEs showed resistance toward spending on compliance. A few participants had no idea about the costs due to unidentified requirements or estimation difficulties. However, participants from the financial sector stated that the compliance process could improve customer trust, making it an investment.

*4.5.2 Compliance costs are challenging to account for.* Participants from government organizations highlighted that they lack sufficient budgets for privacy compliance implementation due to a lack of management support and a strict budget approval process. P06 said, *"As a government organization, we will not get a budget allocated this year for a circular that was issued in the beginning of this year."* However, almost all interviewees from the financial sector have already allocated a budget for PDPA implementation, irrespective of whether they represent the government or the private sector.

In contrast, almost all large corporations in the private sector have allocated a budget for compliance implementation. For most other organizations, the need was present, but the allocation may not have yet been made. However, a few private organizations, mostly smaller enterprises and startups, struggled to understand the breadth and depth of the engagement required to estimate and allocate budgets.

*4.5.3 Cost of implementation is distributed across technical, people, and recurrent aspects.* Almost all participants said that technical improvements would cost them the most, requiring spending on tools, software updates, and information security controls, among others. Additionally, hiring experts will incur a significant cost. Some participants noted an additional cost toward human resources, such as training and awareness. Furthermore, most participants are aware of recurrent costs due to compliance, such as regular audits and maintenance. In contrast, participants from the financial sector do not consider these an additional burden because they are customary in their domain.

# 5 Discussion

Our stakeholder interviews about Sri Lanka's Personal Data Protection Act surfaced a range of experiences and challenges that participants encountered while preparing for the Act's implementation.

*Many challenges match developed countries.* Many of the barriers observed by our participants in Sri Lanka closely mirror those reported in developed countries by prior literature. For example, stakeholder concerns about possible impact on product offerings, growth, and scaling of businesses can also be found in studies on developed countries [43, 48, 63]. Another challenge commonly identified in post-enforcement studies of GDPR compliance, as well as our own, is that legal experts often lack technical knowledge, while technical experts struggle to parse legal interpretations [16, 25, 39, 54, 63]. Prior research has similarly documented compliance challenges stemming from outdated software and technologies [11]. Observing these parallels is critical, as it demonstrates that prior findings often transcend borders and specific laws, suggesting that developing and developed countries can learn from each other's experiences implementing privacy regulations.

## 5.1 Opportunities for improvement

*Communication is key.* Communication emerged as a notable challenge common to both Sri Lanka and prior contexts. Prior research has documented communication breakdowns in various forms, for example many GDPR implementers felt that authorities provided insufficient guidance and support [39, 50, 63]. In

PREPRINT

our study, this manifested as a low level of awareness and understanding among participants about the PDPA and the meaning of its individual provisions. Many participants heavily criticized the DPA's communication strategies, not only in a lack of awareness campaigns about the need to comply, but also the authority's ability to provide clarifying answers when requested (4.2.2). While some uncertainty is expected prior to enforcement [50], minimizing outstanding questions beforehand facilitates smoother implementation. We therefore recommend that regulators, including the DPA, adopt a more proactive communication approach. When asked what resources they relied on, no stakeholders mentioned official DPA documentation. A clear improvement for the DPA and other regulators would be to provide a centralized, easily accessible knowledge base for implementers. Our participants further recommended that such resources should be tailored to address the various distinct needs of specific economic sectors and organizational roles.

For the communication to be effective, it should also be bidirectional. Regulators should not merely broadcast information to stakeholders; they must also actively solicit feedback on the ongoing challenges that implementers encounter. This would allow them to proactively identify and address issues such as believing security controls to be privacy, complexities in the Act, and lack of domain specific guidelines. Regulators could facilitate this through structured surveys, focus groups, or dedicated liaisons.

*Expertise needs to be bootstrapped.* While present in developed nations, some challenges are significantly exacerbated in developing countries, which have limited resources. One acute problem is the shortage of experts in both the legal and technical domains, and especially those possessing cross-disciplinary expertise. Other developing countries such as Nigeria have also reported similar shortages [33]. In smaller, less-resourced countries, the talent pool is naturally smaller, and established educational pathways to develop this expertise may be altogether absent.

Currently, organizations cope by hiring external consultants and attempting to develop in-house expertise on a best-effort basis. They may use prior regulatory compliance efforts as blueprints for newer ones, such as leveraging existing ISO 27001 compliance workflows. In the absence of country-specific resources, organizations may also turn to public documentation designed for other jurisdictions. For instance, without PDPA-specific guides, they may rely on those written about the GDPR.

However, this lack of targeted expertise and understanding can lead implementers astray. We observed many organizations narrowly focusing on data security while neglecting the individual privacy rights that are a central component of the PDPA. This misunderstanding may lead them to adopt inappropriate compliance models. Implementers must be explicitly informed that personal data protection entails more than security controls and extends far beyond standard financial security frameworks, like in ISO 27001 and SOC 2.

It is crucial for regulators to anticipate this behavior. In addition to directly addressing common misconceptions, they should assume that implementers will draw on any resource they can find, including following foreign frameworks, and therefore should clearly document where local regulations diverge from international counterparts. Regulators should also explicitly budget and plan for building domestic expertise through international exchange programs for workforce development or by directly training professionals to seed the local market with experts. Implementers can then rely on this local talent pool when planning their own compliance actions.

## 5.2 Risks to success

*Lack of digitalization creates complexity.* One assumption that may be implicit in prior examples of privacy law implementations from developed countries is that data flows are largely electronic. Our interviews reveal that, frequently, this assumption does not hold in Sri Lanka, where many business processes occur partially or entirely on paper. Paper processes are not fundamentally incompatible with data subject rights like access, rectification, or deletion; however, enabling the exercise of these rights in the physical world is distinct and more challenging. Rather than relying on automated database queries, paper management necessarily requires manual workflows and human-in-the-loop processing. Regulators can assist by forewarning organizations about these scenarios and establishing clear best practices for executing privacy rights across paper-based workflows.

Notably, many paper-based workflows are particularly prevalent in government settings or due to government-mandated processes like auditing, which may have legal requirements involving paper documentation (4.4.2). Therefore, lawmakers concerned that paper processes will impede privacy implementation may be well-positioned to encourage reduced reliance on paper by driving structural change. On the other hand, such efforts might themselves have drawbacks, for example due do the digitalization, connectivity, and literacy issues seen in rural areas (§4.4.1). Therefore, even if providing process-specific guidelines is not feasible, data protection authorities should consider publishing guidelines that account for paper-based processes.

*Careless implementation risks exacerbating inequities.* One characteristic of Sri Lanka common to many other developing nations is the uneven digitalization across different geographic regions [30]. Urban centers like Colombo feature higher population densities, concentrated commercial activity, and higher average digital education levels. They consequently benefit from greater technological access and digital literacy. Conversely, rural areas often lack these advantages, leading to a heavier reliance on traditional, paper-based processes. Participants described how infrastructure deficits and limited digital literacy in rural areas have forced staff to interact with systems on behalf of end users (4.4.1). (Similar intermediary practices have been observed in African countries [34].) Given these geographic disparities, rigid enforcement of technical privacy controls could disproportionately harm those with limited digital access, potentially jeopardizing their ability to utilize crucial services.

*Informal processes create undocumented risks.* Informal processes, such as staff interacting with systems on behalf of end users, represent distinct challenges for privacy compliance. Another example

PREPRINT

uncovered in our interviews is the reliance on informal administrative aides ("peons"), who are frequently tasked with making photocopies, physically transferring documents between departments, and other logistical chores. While serving in an official capacity, their specific interactions with data are rarely documented, despite them having routine physical access to PII. From a data protection perspective, this widespread undocumented access creates security and privacy concerns. If these informal roles remain unaccounted for, and the processes are not audited, these vulnerabilities are likely to persist even after regulations are technically implemented.

*Process visibility as a prerequisite and consequence of regulation.* The undocumented role of peons highlights a broader challenge for privacy regulation implementers. Effectively implementing safe data handling and verifiable data subject rights requires a comprehensive mapping of all existing data flows. This can prove challenging when organizational processes are informal, ad hoc, or disjointed, such as when departments use disjoint parallel systems to achieve the same goals. While this fragmentation is not unique to developing economies, it may be more frequently encountered there [36][53]. Regulators and implementers should be aware that obtaining this visibility is a prerequisite for successful compliance, and budget time accordingly.

On the flip side, our participants' experiences show that increased visibility into processes can emerge as a side effect of attempting to implement regulations. For example, it helped our interviewees identify insecure legacy practices, such as developers relying on personal systems and having unrestricted access to PII. In this way, privacy regulations can serve as a forcing function, compelling organizations to reevaluate their processes and potentially even providing leverage to renegotiate data-sharing relationships with third-party vendors.

*Implementers' expectations for enforcement drive decisions.* Just as privacy implementation can be set back by a lack of visibility into informal workflows, the regulatory environment itself can be opaque and harbor informal processes that hinder implementation. A critical factor in compliance behavior is the perceived credibility of the regulator, determined by their track record reliability in meeting deadlines, transparency in appointing officials, and fairness in applying penalties across organizations of all sizes. The broader societal context is also influential. A volatile legislative environment, where regulations are routinely amended or overturned with lobbying, encourages covered entities to seek political workarounds rather than invest in compliance. So too does pliable legal system where corruption is endemic. Organizations are especially likely to exploit these alternative pathways when they view privacy compliance purely as a cost, offering no intrinsic business value and driven by little to no consumer demand.

## 5.3 Culture as linchpin

*Culture may conflict with privacy.* Multiple interviewees described Sri Lanka as having an inherently open culture where freely sharing personal information is normalized. By itself, this openness does not conflict with privacy, since frameworks like contextual integrity conceptualize privacy in terms of societal norms and expectations [37], which can vary widely in their permissiveness. Nonetheless, operationalizing strict privacy rights, such as those mandated by the PDPA and GDPR, almost necessarily entails imposing stronger access controls which may conflict with informal sharing norms. As we documented, revoking previously-held access can alienate employees, who may interpret these new technical restrictions as a signal that they are not deemed trustworthy. Research has documented similar interpersonal tensions surrounding security implementations in other open cultures [23]. For end users, rigid access controls may impede the ad hoc sharing behaviors they historically relied on. This tension may even call for rethinking how certain privacy rights are operationalized, perhaps by architecting explicit mechanisms for authorized sharing and delegation that respect and accommodate the local cultural context.

*Public demand may be an insufficient motivator.* Several interviewees believed that Sri Lanka's open culture results in limited public demand for data protection rights, so accommodating them yields negligible competitive advantage (4.3). Future research should investigate this assumption empirically, as it may not be true. Currently, Sri Lankans have few opportunities to demonstrate a preference for privacy-protective services, as they often lack meaningful choices and alternatives when their data is collected. (In light of the country's financial crises, citizens also understandably prioritize immediate economic concerns over abstract data rights.) Still, this dynamic highlights that public demand alone is insufficient to incentivize corporate privacy initiatives; governments must couple legislation with robust auditing and enforcement mechanisms. Absent strict regulatory incentives, organizations are unlikely to proactively implement costly privacy architectures. This also suggests that Sri Lanka and countries with similar cultures may benefit from privacy education initiatives to inform citizens about their rights and the tangible value that privacy can provide for them. Doing so may require reaching across the digital divide. For example, privacy advocates can use existing communication infrastructure such as radio-based public service announcements to reach out to rural areas and populations with lower digital literacy.

*A glass half full.* In some respects, our analysis of the PDPA's pre-implementation phase paints a pessimistic picture. Many organizations have yet to begin implementation, and some remain entirely unaware of their legal obligations. For those actively planning, compliance costs are accruing due to the need for specialized consultants and systemic re-engineering. Yet, from their perspective, the return on investment remains unclear given the perceived lack of public demand. The possibility of legislative amendments and the availability of loopholes may lead organizations to continued avoidance and indefinite delays. Worse, there is some risk that implementation devolves into "privacy theater"—pro forma rituals undertaken merely to simulate compliance, lacking actual benefits for privacy due to informal workarounds. If unmanaged, this risks souring the population on the general notion of privacy—a concept that is already less structurally embedded in Sri Lanka than in other cultures.

On the other hand, we see the situation as not necessarily that dire and the challenges as not insurmountable. Many organizations have made substantive progress toward compliance, particularly within the financial sector, which has a greater track record of

PREPRINT

compliance with regulations due to the long-standing authority of the CBSL, which has explicitly emphasized consumer-privacy compliance in its directives [6]. While significant barriers remain, many are concentrated within government organizations—a sector often exempted from comparable regulations, such as the CCPA. Furthermore, the PDPA's implementation is already spurring improvements in organizational security policies, which are a critical complement to privacy rights. Finally, the presence of the regulation, and the need to comply with it, is successfully prompting necessary societal conversations about the intrinsic value of data protection.

When the PDPA finally goes into effect, it will not be the end of the compliance process, but neither will it be the beginning. As our findings show, the pre-implementation phase is a crucial moment in the regulatory lifecycle. By heeding the lessons of the PDPA in Sri Lanka, other countries can navigate a smoother journey toward comprehensive privacy protection.

## 6 Conclusion

Sri Lanka, a developing country in South Asia, is preparing to enforce its first privacy regulation, the Personal Data Protection Act, which is largely similar to Europe's GDPR. This offered us a unique opportunity to study the challenges of implementing privacy regulations as they are happening, in contrast with most research, which does so retroactively. Sri Lanka's status as a developing country further increases the potential for findings to transfer to other Majority World countries that have not yet enacted privacy laws. We conducted 35 interviews with stakeholders of government and private organizations of varying sizes. While years had passed since the Act was enacted, most organizations were at the very early stage of compliance implementation, although financial organizations were well ahead, likely due to greater compliance expertise and guidance from the Central Bank of Sri Lanka. We found that many of the challenges implementers are experiencing match those of developed countries, while others are likely more specific to developing countries: severely underdeveloped infrastructure, non-digitized systems, and the reliance on aides ("peons") for carrying out routine tasks, which may expose these workers to sensitive documents. Many of the challenges centered on the difficulties of developing a privacy-forward organizational culture, with appropriate buy-in from leadership; some participants attributed this to Sri Lanka's national culture being open and trusting. Our results offer lessons for future regulators and implementers, who may consider steps such as staged compliance and iterative improvements to the legislation—approaches that may benefit stakeholders as well as regulators themselves.

## Acknowledgments

We would like to thank Primal Wijesekera, without whom this project would not have happened. We thank W.A.C. Weerakoon for exceptional help with the ground-level logistics of this project and invaluable encouragement during the course of this study. We are also grateful to our participants, whose time and insights helped shed light on this important topic.

## References

[1] Nitin Agrawal, Reuben Binns, Max Van Kleek, Kim Laine, and Nigel Shadbolt. 2021. Exploring Design and Governance Challenges in the Development of Privacy-Preserving Computation. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–13. doi:10.1145/3411764.3445677

[2] Oshrat Ayalon, Eran Toch, Irit Hadar, and Michael Birnhack. 2017. How Developers Make Design Decisions about Users' Privacy: The Place of Professional Communities and Organizational Climate. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. ACM, New York, NY, USA, 135–138. doi:10.1145/3022198.3026326

[3] Anu Bradford. 2020. *The Brussels Effect: How the European Union Rules the World*. Oxford University Press, Oxford, UK. doi:10.1093/oso/9780190088583.001.0001

[4] Virginia Braun and Victoria Clarke. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. doi:10.1191/1478088706qp063oa

[5] California. 2018. The California Consumer Privacy Act of 2018. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[6] Central Bank of Sri Lanka. 2023. Financial Consumer Protection Regulations, No. 01 of 2023. Government Gazette Extraordinary No. 2344/17, 9 August 2023. https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/fcrd_regulations_no_01_of_2023_e.pdf

[7] Anupam Chander, Meaza Abraham, Sandeep Chandy, Yuan Fang, Dayoung Park, and Isabel Yu. 2021. Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation. *SSRN Electronic Journal* (2021). doi:10.2139/ssrn.3827228

[8] Wenhong Chen, Gejun Huang, Joshua Miller, Kye-Hyoung Lee, Daniel Mauro, Bryan Stephens, and Xiaoqian Li. 2018. "As We Grow, It Will Become a Priority": American Mobile Start-Ups' Privacy Practices. *American Behavioral Scientist* 62, 10 (Sept. 2018), 1338–1355. doi:10.1177/0002764218787867

[9] Data Protection Authority Sri Lanka. 2025. Data Protection Authority Sri Lanka. https://www.dpa.gov.lk/.

[10] Department of Census and Statistics, Ministry of Finance, Planning and Economic Development, Sri Lanka. 2024. Census of Population and Housing 2024. https://www.statistics.gov.lk/Resource/en/Population/CPH_2024/Population_Preliminary_Report.pdf.

[11] Leon Wipp Ekman and Petter Billgren. 2017. *Compliance Challenges with the General Data Protection Regulation*. Master's thesis. Lund University. https://lup.lub.lu.se/student-papers/search/publication/8911983.

[12] European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance). https://data.europa.eu/eli/reg/2016/679/oj.

[13] Ming Fan, Le Yu, Sen Chen, Hao Zhou, Xiapu Luo, Shuyue Li, Yang Liu, Jun Liu, and Ting Liu. 2020. An Empirical Evaluation of GDPR Compliance Violations in Android mHealth Apps. In *2020 IEEE 31st International Symposium on Software Reliability Engineering (ISSRE)*. IEEE, 253–264. doi:10.1109/ISSRE5003.2020.00032

[14] Graham Greenleaf. 2023. Global Data Privacy Laws 2023: 162 National Laws and 20 Bills. *Privacy Laws & Business International Report* 181 (2023), 1–4. https://ssrn.com/abstract=4426146.

[15] Graham Greenleaf. 2025. Global Data Privacy Laws 2025: 172 Countries, Twelve New in 2023/24. https://papers.ssrn.com/abstract=5275559. social science research network:5275559 doi:10.2139/ssrn.5275559

[16] Sukhi Gulati-Gilbert. 2023. *Privacy Law in Practice: Exploring Challenges to Modern Privacy Compliance*. Master's thesis. Massachusetts Institute of Technology. https://hdl.handle.net/1721.1/151849.

[17] Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. 2018. Privacy by Designers: Software Developers' Privacy Mindset. *Empirical Software Engineering* 23, 1 (Feb. 2018), 259–289. doi:10.1007/s10664-017-9517-1

[18] Indonesian Government. 2022. Personal Data Protection Law (Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022). Republic of Indonesia.

[19] International Monetary Fund. 2023. *Sri Lanka: Request for an Extended Arrangement Under the Extended Fund Facility*. Technical Report 2023/116. International Monetary Fund, Washington, D.C. doi:10.5089/9798400238987.002

[20] Yana Chaeru Taufik Ismail and Arwansyah bin Kirin. 2025. Digital Privacy and Personal Data Protection in Southeast Asia: Challenges and Efforts toward Legal Harmonization. *Justitia Nova: Indonesian Journal of Modern Law* 1, 1 (June 2025), 24–34. https://ejournal.kampusalazhar.ac.id/index.php/jnova/article/view/169/235.

[21] Loso Judijanto, Nuryati Solapari, and Irman Putra. 2024. An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. *The Easta Journal Law and Human Rights* 3, 01 (Oct. 2024), 20–29. doi:10.58812/eslhr.v3i01.351

PREPRINT

[22] Navid Kagalwalla, Tanvi Garg, Prathamesh Churi, and Ambika Pawar. 2019. A Survey on Implementing Privacy in Healthcare: An Indian Perspective. *International Journal of Advanced Trends in Computer Science and Engineering* 8, 3 (June 2019), 963–982. doi:10.30534/ijatcse/2019/97832019

[23] Judith Kankam-Boateng, Marco Peressotti, Jan Stentoft, Kent Adsbøll Wickstrøm, Vincent Charles Keating, Louise Alison Tumchewics, Olivier Schmitt, Amelie Theussen, and Peter Mayer. 2026. 'It's Confusing, Insecure, and Messy' – Mapping the Gaps Between Stakeholders' Cybersecurity Mental Models in the Danish Defence Sector. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*. ACM, Barcelona Spain, 1–26. doi:10.1145/3772318.3791032

[24] Alexandra Klymenko, Stephen Meisenbacher, Luca Favaro, and Florian Matthes. 2025. Supporting the Integration of Privacy-Enhancing Technologies into the Software Development Life Cycle. *SN Computer Science* 6, 6 (2025), 592. doi:10.1007/s42979-025-04127-6

[25] Oleksandra Klymenko, Stephen Meisenbacher, and Florian Matthes. 2023. Identifying Practical Challenges in the Implementation of Technical Measures for Data Privacy Compliance. In *Proceedings of the 29th Americas Conference on Information Systems (AMCIS 2023)*. Association for Information Systems. https://aisel.aisnet.org/amcis2023/sig_sec/sig_sec/2/.

[26] Ze Shi Li, Colin M. Werner, Neil A. Ernst, and Daniela E. Herlea Damian. 2022. Towards Privacy Compliance: A Design Science Study in a Small Organization. *Information and Software Technology* 146 (2022), 106868. doi:10.1016/j.infsof.2022.106868

[27] Zengrui Liu, Umar Iqbal, and Nitesh Saxena. 2024. Opted Out, Yet Tracked: Are Regulations Enough to Protect Your Privacy? *Proceedings on Privacy Enhancing Technologies* 2024, 1 (Jan. 2024), 280–299. doi:10.56553/popets-2024-0016

[28] A. Lonzetta and T. Hayajneh. 2018. Challenges of Complying with Data Protection and Privacy Regulations. *ICST Transactions on Scalable Information Systems* (July 2018), 166352. doi:10.4108/eai.26-5-2020.166352

[29] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 23 pages. doi:10.1145/3359174

[30] Md Aslam Mia, Md Imran Hossain, and Sunil Sangwan. 2024. Determinants of Digitalization: Evidence from Asia and the Pacific Countries. *Digital Transformation and Society* 3, 4 (March 2024), 340–358. doi:10.1108/DTS-10-2023-0097

[31] Ministry of Finance, Planning and Economic Development, Sri Lanka. 2022. Interim Policy Regarding the Servicing of Sri Lanka's External Public Debt. https://www.treasury.gov.lk/api/file/54a19fda-b219-4dd4-91a7-b3e74b9cd683.

[32] Anamarija Mladinić, Zdravko Vukić, and Ante Rončević. 2023. GDPR Compliance Challenges in Croatian Micro, Small and Medium Sized Enterprises. *Pravni vjesnik* 39, 3-4 (Dec. 2023), 53–75. doi:10.25234/pv/23972

[33] Yahya Umar Muhammad, Ibrahim Abubakar, and Eli Adama Jiya. 2026. Data Sovereignty and the Leaky Pipe: Charting a Course for Data Governance and Information Security in Nigeria and Africa. *Journal of Basics and Applied Sciences Research (JOBASR)* 4, 2 (2026), 224–232. doi:10.4314/jobasr.v4i2.23

[34] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. 2023. "In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 570–587. doi:10.1109/SP46215.2023.10179410

[35] National Data Protection Authority (ANPD). 2018. Brazilian Data Protection Law No. 13,709 of August 14, 2018.

[36] T. N. Nguyen. 2023. Developing health information systems in developing countries: Lessons learnt from a longitudinal action research study in Vietnam. *The Electronic Journal of Information Systems in Developing Countries* 89, 5 (2023), e12268. doi:10.1002/isd2.12268

[37] Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books, Stanford, CA, USA. doi:10.1515/9780804772891

[38] Razieh Nokhbeh Zaeem and K. Suzanne Barber. 2020. The Effect of the GDPR on Privacy Policies. *ACM Transactions on Management Information Systems* 12, 1 (Dec. 2020), 1–20. doi:10.1145/3389685

[39] Chris Norval, Heleen Janssen, Jennifer Cobbe, and Jatinder Singh. 2021. Data Protection and Tech Startups: The Need for Attention, Support, and Scrutiny. *Policy & Internet* 13, 2 (June 2021), 278–299. doi:10.1002/poi3.255

[40] Parliament of the Democratic Socialist Republic of Sri Lanka. 2022. Personal Data Protection Act, No. 9 of 2022. https://www.documents.gov.lk/view/acts/2022/3/09-2022_E.pdf.

[41] Parliament of the Democratic Socialist Republic of Sri Lanka. 2025. Personal Data Protection (Amendment) Act, No. 22 of 2025. https://www.parliament.lk/uploads/acts/gbills/english/6384.pdf.

[42] Parliament Secretariat Sri Lanka. 2022. The Constitution of the Democratic Socialist Republic of Sri Lanka. https://www.parliament.lk/files/pdf/constitution.pdf.

[43] Nazar Poritskiy, Flávio Oliveira, and Fernando Almeida. 2019. The Benefits and Challenges of General Data Protection Regulation for the Information Technology Sector. *Digital Policy, Regulation and Governance* 21, 5 (Aug. 2019), 510–524. doi:10.1108/DPRG-05-2019-0039

[44] Budi Prasetyo, I Gusti Ayu Ketut Rachmi Handayani, and Adi Sulistiyono. 2025. Data Protection Laws in Indonesia: Navigating Privacy in the Digital Age. *SIDE: Scientific Development Journal* 2, 1 (2025), 9–16. doi:10.59613/petfxv64

[45] Sammani Rajapaksha, Panu Puhtila, Timi Heino, and Sampsa Rauti. 2024. A Comparative Study of Finnish and Sri Lankan Privacy Regulations and Compliance on the Web. In *Proceedings of the 2024 9th International Conference on Information Systems Engineering*. ACM, Chiang Mai, Thailand, 41–48. doi:10.1145/3711954.3711957

[46] Kiki Rezki Ramadhan and Chandra Wijaya. 2022. The Challenges of Personal Data Protection Policy in Indonesia: Lesson Learned from the European Union, Singapore, and Malaysia. *Technium Social Sciences Journal* 36 (2022), 18–28. doi:10.47577/tssj.v36i1.7442

[47] Fachrul Razi, Hadi Tuasikal, and Dwi Pratiwi Markus. 2024. Implementation and Challenges of the Personal Data Protection Law in Indonesia. *Indonesian Journal of Social Technology* 5, 12 (Dec. 2024), 6015–6021. doi:10.59141/jist.v5i12.1285

[48] Fabian Schäfer, Heiko Gebauer, Christoph Gröger, Oliver Gassmann, and Felix Wortmann. 2023. Data-Driven Business and Data Privacy: Challenges and Measures for Product-Based Companies. *Business Horizons* 66, 4 (July 2023), 493–504. doi:10.1016/j.bushor.2022.10.002

[49] Awanthika Senarath and Nalin A. G. Arachchilage. 2018. Why Developers Cannot Embed Privacy into Software Systems?: An Empirical Investigation. In *Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018*. ACM, Christchurch, New Zealand, 211–216. doi:10.1145/3210459.3210484

[50] Sean Sirur, Jason R.C. Nurse, and Helena Webb. 2018. 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*. ACM, Toronto Canada, 88–95. doi:10.1145/3267357.3267368

[51] Yelena Smirnova and Victoriano Travieso-Morales. 2024. Understanding Challenges of GDPR Implementation in Business Enterprises: A Systematic Literature Review. *International Journal of Law and Management* 66, 3 (April 2024), 326–344. doi:10.1108/IJLMA-08-2023-0170

[52] Sarah Spiekermann, Jana Korunovska, and Marc Langheinrich. 2019. Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers. *Proc. IEEE* 107, 3 (March 2019), 600–615. doi:10.1109/JPROC.2018.2866769

[53] Angelique Spierings, Don Kerr, and Luke Houghton. 2017. Issues that support the creation of ICT workarounds: Towards a theoretical understanding of feral information systems. *Information Systems Journal* 27, 6 (2017), 775–794. doi:10.1111/isj.12123

[54] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama, Japan, 1–15. doi:10.1145/3411764.3445768

[55] Attamongkol Tantratian and Eka Nugraha Putra. 2025. Data Protection in Thailand and Indonesia: Struggling and Striving for European-Like Privacy. doi:10.2139/ssrn.5341565

[56] Thailand. 2019. Personal Data Protection Act B.E. 2562 (2019) (English Version). https://data.thailand.opendevelopmentmekong.net/en/laws_record/2562/resource/ec616be5-9fbf-4071-b4b5-cb1f3e46e826.

[57] Kenneth Thilakarathna, Sachintha Pitigala, Jayantha Fernando, and Primal Wijesekera. 2024. Empirical Analysis of Sri Lankan Mobile Health Ecosystem: A Precursor to an Effective Stakeholder Engagement. In *The 24th Privacy Enhancing Technologies Symposium (PETS), Workshop on Privacy, Safety, and Trust in Mobile Health Apps*. Bristol, UK. https://arxiv.org/abs/2407.13415.

[58] Nik Thompson, Tanya McGill, Anna Bunn, and Rukshan Alexander. 2020. Cultural Factors and the Role of Privacy Concerns in Acceptance of Government Surveillance. *Journal of the Association for Information Science and Technology* 71, 10 (2020), 1129–1142. doi:10.1002/asi.24372

[59] Transparency International. 2025. Corruption Perceptions Index (CPI) 2025. https://www.transparency.org/en/cpi/2025/index/lka.

[60] UNCTAD. 2025. *Data Protection and Privacy Legislation Worldwide*. Technical Report. United Nations Conference on Trade and Development. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[61] Thomas Serban von Davier, Konrad Kollnig, Reuben Binns, Max Van Kleek, and Nigel Shadbolt. 2023. We Are Not There Yet: The Implications of Insufficient Knowledge Management for Organisational Compliance. doi:10.48550/arXiv.2305.04061

[62] World Bank Group. 2025. Data for Sri Lanka, Lower Middle Income. https://data.worldbank.org/?locations=LK-XN.

[63] Nemer Alberto Zaguir, Guilherme Henrique De Magalhães, and Mauro De Mesquita Spinola. 2024. Challenges and Enablers for GDPR Compliance: Systematic Literature Review and Future Research Directions. *IEEE access : practical innovations, open solutions* 12 (2024), 81608–81630. doi:10.1109/ACCESS.2024.3406724


PREPRINT

# A Open science

For the reproducibility of the study, we have included our interview questionnaire and the thematic analysis codebook below.

## A.1 Interview questionnaire

We are conducting research to understand how stakeholders in Sri Lanka approach their Personal Data Protection Act (PDPA) compliance requirements. The study focuses on the processes, challenges, costs, perceived responsibilities, and stakeholder roles. The objective is to identify effective strategies for regulatory roll-out and adoption.

*At what stage is your organization in the PDPA compliance process?*

(1) Haven't thought about it yet
(2) In the planning phase
(3) In the middle of implementing required tasks
(4) Have finished the implementation to become fully compliant

Remaining questions were adjusted according to the compliance stage of the organization.

*RQ: How do organizations and personnel plan to prepare for the upcoming regulations and what is the current state?*

- How [do you plan to] / [did you] find out what you need to do to become compliant?
- Have you identified the required expertise to implement the compliance? What roles [will] / [did] they play in your compliance process?
- Do you already have the expertise required to implement compliance within your organization? How [do you plan to] / [did you] obtain the expertise?
- Have you identified any additional resources that may be needed for the compliance implementation?
- Can you briefly describe [how you plan] / [what you are doing] to comply with PDPA?

*RQ: What is the role of the regulators in helping organizations?*

- Is the information provided by the regulator sufficient to make decisions on the implementation of PDPA compliance?
- What information did you follow?
- Did you have any instances where you needed to get clarification from the regulator? If you reached out to them, did it help?
- What information from the regulator would have made your PDPA compliance planning and implementation easier?
- How do you think the regulator should be involved in PDPA compliance planning and implementation?

*RQ: What is the role of cultural norms?*

- Is there anything about your experiences that you think is specific to your company?
- Is there anything about your experiences that you think would be different in another country?
- What do you think others should know about the process of complying with privacy laws?
- Sometimes, when a new law like this is passed, it is not enough to implement specific technical solutions, but rather the mindset or attitudes need to change. Do you think there are such changes that the PDPA requires?
- What are the specific things you think need to be changed from an organizational, cultural, and personnel perspective?

*RQ: What are the technical challenges that stakeholders come across?*

- (If they have not even thought about PDPA) what keeps you waiting to start compliance implementation?
- What was the most challenging task until now? And is it still a challenge or how have you overcome it?
- Out of the tasks ahead, which tasks do you think will be the most challenging? How do you plan or prepare to face it?
- What challenges do you think require a big change in the organization for the compliance process? What is the big change? Why is that change required? How do you plan to implement the change?

*RQ: How do the stakeholders perceive the cost and budget of implementation?*

- What do you think about the costs of having to comply with PDPA?
- Do you foresee any indirect costs of the implementation of PDPA compliance?
- Do you foresee any benefits of the implementation of PDPA compliance?
- What are the costs of maintaining PDPA compliance?

## A.2 Interview codebook

The codebook can be found in the supplementary materials: https://osf.io/yp95h/overview?view_only=de4cf9acb273417781ddad0d15a3b85a

# B Ethical considerations

Ethical standards were maintained throughout the research process. Informed consent was obtained from all participants, and they were informed about the objectives of the study, its voluntary nature, and confidentiality measures. Our participants were not compensated. Given that all our participants were well-paid professionals for whom participation in our study was not a financial burden, payments can be considered culturally inappropriate; typical amounts could be seen as insulting and might dissuade rather than encourage participation, while proportionately higher ones may be considered biasing or even coercive. The primary risk we identified was a breach of confidentiality that may cause embarrassment or reputational damage to participants or their organizations. We mitigated this by keeping participants anonymous, not audio-recording conversations, and avoiding records that could link research data to identities. All anonymized data was stored securely with only authorized research team members having access to it. Ethical approval for the study was obtained from the Ethics Review Committee of the affiliated institution.

PREPRINT