A Comparative Study of Finnish and Sri Lankan Privacy Regulations and Compliance on the Web

Sammani Rajapaksha
University of Turku
Turku, Finland
syraja@utu.fi

Panu Puhtila
University of Turku
Turku, Finland
papuht@utu.fi

Timi Heino
University of Turku
Turku, Finland
tdhein@utu.fi

Sampsa Rauti
University of Turku
Turku, Finland
sjprau@utu.fi

Abstract

With the increase in various risks for website user privacy in the recent decade, the regulators across the globe have stepped up and brought forth new legislation to better safeguard against privacy violations, to varying degrees. Mandates such as the European GDPR require the websites to comply with certain standards of privacy, such as obtaining a freely given consent for data processing. However, in many countries, these kinds of privacy enhancing practices are not employed. In this paper, we conduct a comparative analysis of several privacy aspects between Sri Lankan and Finnish websites, to determine what differences exist between them and how the regulations are implemented between these two countries. Our survey includes 94 Sri Lankan public sector websites, 16 Sri Lankan private company websites, 63 Finnish public sector websites and 15 Finnish private company websites. The public sector websites we studied presented the governmental institutions in these countries, and the private company websites presented the largest domestic corporations measured by revenue. Based on the concepts derived from the regulation with open coding, we also measure the privacy aspects in eight categories: (1) use of cookie consent banner, (2) availability of privacy policy, (3) privacy policy readability, (4) use of HTTPS, (5) number of third parties receiving personal data from the website, (6) cross-border data transmissions, (7) use of dark patterns in cookie consent banner and (8) availability of the website. We also conducted a readability analysis on the privacy policies used in the websites that had them. Our results show that the Finnish websites generally fared well in terms of privacy and compliance. In Sri Lanka, 1) government websites fared worse than private companies and 2) all websites had more problems in terms of privacy than the Finnish ones. This points to the effectiveness of GDPR and well-enforced legislation in general, in improving privacy matters.

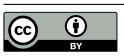
CCS Concepts

• **Security and privacy → Web application security**.

Keywords

Regulation, websites, online privacy, data leaks, dark patterns

ACM Reference Format:
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 *2024 9th International Conference on Information Systems Engineering (ICISE 2024), December 14–16, 2024, Chiang Mai, Thailand.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3711954.3711957



ICISE 2024, Chiang Mai, Thailand

ACM ISBN 979-8-4007-1736-9/24/12
https://doi.org/10.1145/3711954.3711957

1 Introduction

Web services have become a common way to carry out all kinds of everyday tasks in recent years. Privacy is an important issue in such essential services. To guarantee users' privacy, several different privacy regulations aim to protect personal data and give people control of how their data is being processed. By ensuring that users consent to data collection and can obtain sufficient information on data processing activities, privacy regulations increase accountability and make handling users' personal data fairer and transparent. Many consider the GDPR the most thorough and strict privacy law.

Many countries have modeled their data protection acts after the GDPR, and Sri Lanka was the first to do so in South Asia, as the Personal Data Protection act (PDPA) was enacted in 2022. Both the GDPR and the PDPA are concerned with lawful, fair and transparent data processing and advocate the privacy-by-design approach. They define several obligations for data controllers and rights for data subjects. They seek to ensure data accuracy, integrity and confidentiality, while data collection purposes and storage are limited. Limitations are also put on processing of special category data and international data transfers. Unfortunately, however, there is often a large gap between the law and actual practical implementation and enforcement of privacy regulation. Web developers and website owners have to know how to apply the privacy regulations in practice and how to make their websites compliant.

In this paper, we extract privacy related quality attributes and actual implementation from the privacy regulations, and study how well these requirements are met in different websites in practice. As case studies, we have chosen to analyze both governmental and company websites in two countries: Finland and Sri Lanka. This allows for an interesting comparison between a European country with the GDPR and a longer history of online privacy regulation, and a South Asian country that has introduced a comprehensive

privacy regulation only much more recently. Based on this, the following research questions were formulated:

- **RQ1**: What practical software privacy related measures do the analyzed regulations require in terms of implementation?
- **RQ2**: How do these differ between the two studied countries?
- **RQ3**: How well are these requirements followed in practice on government and company websites in the studied countries?

The rest of the paper is organized as follows. Section 2 reviews the related work. Section 3 explains the selection process of the studied privacy regulations, the extraction of the concept from the legal texts, and the process of studying the practical compliance with the regulation in the web environment. Section 4 discusses both theoretical results of conceptual regulation analysis and findings of the empirical website survey. Section 5 covers the implications of our findings, and Section 6 concludes the paper.

2 Related Work

The study by Sooriyabandara [24] focuses on the conflict that exists between the right to privacy and the right to information. It also exemplifies how Sri Lankan law has improved in maintaining the right to information yet lags in upholding the right to privacy. It gives evidence of needing improvement within Sri Lanka's legal system for the right to privacy. The study by Nanayakkara [16] explores the effectiveness of privacy policies in Sri Lanka. Results show that most policies are too long to read and incomprehensible. Although the Sri Lankan laws on privacy show awareness of international standards, there is a need to do more in order to protect consumers' privacy better.

Madugalla [13] compares the legislative landscape of Sri Lanka, in terms of legislation on privacy, to that of other countries such as the United Kingdom and the wider area of Europe. They conclude from this comparison that legislation in Sri Lanka is in dire need of revision in offering privacy protection to its citizens in the modern age. Ratnayake [22] studied obstacles to the use of electronic medical records in Sri Lanka and came to the conclusion that many amendments in the current legislation should be made since, although Sri Lankan law does recognize the validity of electronic records in general, legislation on cybercrimes is inadequate in protecting patients' privacy.

Ranathunga and Wickramarachchi [21] developed a framework to help the Sri Lankan IT-enterprises better comply with GDPR regulations when dealing with clientele based in the EU. Bentototahewa [3] conducted a case study comparing Sri Lankan and United Kingdom privacy legislations, and highlighted that there is an urgent need for more international co-operation in these matters in general as the differences between current national legislations are so great. Rajapaksha et al. [20] investigated the state of Sri Lankan data protection legislation, and came to a conclusion that it needed an urgent update as due to technological progress it failed to answer many issues prevalent in the modern internet. Abeysekara and Ranasinghe [1] have presented a more robust data protection framework for Sri Lankan legislation. Greenleaf [8] discussed the state and advances of data protection laws within the South-East Asia region, making a comparison between Nepal, Pakistan, and Sri Lanka. He concluded that at the time of his writing there was a need to improve this sector. Navaratna [17] examined a state of Sri-Lankan cyber-crime legislation and came to a conclusion that it had a number of loopholes which needed to be fixed to make it more secure. Dissanayaka [7] performed the analysis of readiness of Sri-Lankan legislation and authorities to answer the imminent cyber-threats and in general arrived to conclusion that the level of preparedness was sufficient. Kulathunga [11] compares Sri Lankan and EU cyber-crime and privacy legislation and identifies that Sri Lankan laws are in dire need of being updated to match threats faced in the modern world.

The study by Kautto et al. [10] examines whether Finnish municipalities provide Freedom of Information (FOI) and privacy statements on their websites. The results reveal that such information was absent or difficult to find despite Finland's long tradition of FOI legislation. Heino et al. [9] studied how much personal data 34 Finnish public sector web services transmitted to third-party analytics and how well the transparency of privacy policies. The results showed large discrepancies in many cases between privacy policies and real time data sharing, such as device details not mentioned or user-specific identifiers. Similarly, the research of Puhtila et al. [18] is a good example of data leakage to third parties, where out of 26 Finnish political party websites studied, 19 of them leaked possibly sensitive personal data to third parties, mainly Google and Meta.

There is also lots of research on the social attitudes towards privacy and security in different cultural contexts. An example is a study by Kumaraguru et al. [12], which focuses on qualitative and quantitative data from over 10,000 respondents which in turn reveal widespread misconceptions about privacy protections. Key insights from the research underpin the requirements of policymakers to understand public sentiments for creating effective laws on privacy matched to the unique socio-cultural context of India. Similarly, Martin et al. [14] investigate digital self-expression among South Asians and nationals in Qatar and the UAE. Results indicate that South Asians are more opposed to censorship and more concerned about internet surveillance compared to Qataris and Emiratis. The findings also denote how the values of self-expression in those regions were more a factor of the socio-cultural than the economic factors, with South Asians generally more permissive of privacy and against censorship compared to their counterparts. Furthermore, Cecere et al. [6] examine the variation in the privacy concerns about SNSes across 22,253 individuals in 26 European Union countries, which reveals that cultural values and socio-demographic factors exert strong influences on the concerns, usually showing individualist cultures with lower concern than those of a collectivist nature.

3 Methods

3.1 Selection of privacy regulations

In this study, 5 laws and regulations concerning online privacy in Finland and Sri Lanka were analyzed. Table 1 lists the selected regulations and their current status. The regulations include the EU's General Data Protection Regulation (GDPR), Sri Lanka's Personal Data Protection Act (PDPA), Finland's Data Protection Act (DPA), Sri Lanka's Electronic Transactions Act (ETA), and EU's Directive

Act	Link	State of Enforcement	Country
Personal Data Protection Act, No. 9 of 2022	https://parliament.lk/uploads/acts/gbills/english/6242.pdf	Partially Enforced (2023-2025)	Sri Lanka
Electronic Transactions Act, 2006	https://www.icta.lk/icta-assets/uploads/2016/03/ElectronicTransactionActNo19of2006.pdf	Enforced	Sri Lanka
Data Protection Act, 2018	https://www.finlex.fi/fi/laki/ajantasa/2018/20181050	Enforced	Finland
General Data Protection Regulation, 2016	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679	Enforced	Finland, EU
Directive (EU) 2022/2555	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555	Partially Enforced (2023-2025)	Finland, EU

Table 1: The studied regulations and their states of enforcement.

2022/2555 on cybersecurity (hereafter CSD for Cybersecurity Directive).

The General Data Protection Regulation, commonly referred to as GDPR, is an elaborate European Union data protection law approved in 2016 but officially enforced on May 25, 2018. It is designed to enhance the control of individuals over their personal data and to harmonize data protection laws of Europe. Key elements of the GDPR are a right of an individual to access, rectify, erase their personal data; consent in advance to process personal data; data protection principles; accountability; and privacy by design. This marks a radical change toward accountability and transparency in the processing practices as related to personal data.

Strongly inspired by the GDPR, the Personal Data Protection Act (PDPA) of 2022 is a data protection regulation enacted to ensure the lawful processing of personal data in Sri Lanka. This law regulates the collection, processing, and storage of personal data of individuals. The PDPA is meant for protecting individuals' privacy, defining rights for data subjects, and establishing obligations for data controllers and processors. This regulation is not yet fully enforced at the time of this writing, as some parts will only come into force in March 2025.

As for the other acts we have included here, Sri Lanka's Electronic Transactions Act established a legal framework on e-transactions ensuring the validity and enforceability of electronic records and signatures. This helped the development of better trust in digital transactions. Next, The Data Protection Act 2018 in Finland represents the national implementation of GDPR. It focuses on the processing of personal data and builds up a focus on the protection of the privacy rights of individuals. Finally, Directive (EU) 2022/2555 which has a key objective to make the cybersecurity posture much stronger in the EU. It will, in substance, impose on member states an obligation to establish a framework to improve cybersecurity capabilities from or related to critical sectors like energy, transport, health, and digital infrastructure.

3.2 Conceptual analysis of privacy regulations

To identify parts of the regulations that concern software development and practical compliance, the current study makes use of grounded theory and open coding as presented by Strauss and Corbin [26]. In grounded theory, researchers examine a collection of qualitative data – in the current study, the privacy regulations. From this data, concepts are then derived. In this particular study, this means the actual requirements the analyzed regulations set for software development and implementation.

Open coding involves coding small sections of the text. Concepts are then identified in these sections, and the found concepts are named. We marked all the parts of the regulatory text that were deemed to have implications for software development and implementation. Two authors read the texts and marked the relevant parts. Any disagreements between the two authors were then discussed until consensus was reached. A list of relevant concepts derived from regulations was then created.

3.3 Analyzing privacy issues and compliance on websites

The concepts derived from regulation were used to conduct a practical analysis on the privacy issues and compliance of Finnish and Sri Lankan websites, concentrating on the front end. While all of the found concepts could not be examined in the web environment, we chose the most relevant ones. The analyzed concepts and the process are discussed in more detail in Section 4.2.

Governmental and company websites in both countries were analyzed. To select the websites to be studied, we used listings of Finnish and Sri Lankan government websites [1], as well as lists of the largest companies in both countries [2]. In the end, all 63 government websites from Finland, 15 companies from Finland, all 94 Sri Lankan government websites, and 16 company websites from Sri Lanka were chosen to be included in the study.

The analysis was mostly done manually by examining the relevant privacy and compliance issues on the websites. For example, the cookie consent banners were manually examined. For network

[1] https://www.gov.lk/government/web-sites

[2] See https://www.asiakastieto.fi/yritykset/top-listat, https://www.zoominfo.com/top-lists/top-10-companies-in-LK-by-revenue and https://en.wikipedia.org/wiki/List_of_largest_companies_in_Sri_Lanka

traffic analysis and detecting personal data (e.g. visited URL addresses) potentially leaking to third parties, we used both an automatic tool [5] and Google Chrome developer tools to thoroughly examine the traffic and HTTP request payloads.

4 Results

4.1 Conceptual Analysis

As a result of analyzing the privacy regulations listed in Section 3, we derived several concepts that are central for regulatory compliance. Both more abstract privacy related concepts (such as confidentiality) and the ways to implement them are discussed in this section. The actual privacy enhancing software measures are usually not explicitly mentioned in the regulation. Encryption, anonymization, pseudonymization and access controls are few exceptions.

To start off, many elements usually related to software security, such as the concepts of the CIA triad, are central in the studied privacy regulations. *Confidentiality* is an essential concept in both GDPR and PDPA. It protects data from unauthorized access [29]. It is often implemented by encryption, specifically mentioned in GDPR, PDPA, DPA and SCD. Encryption is often used to guarantee confidential and secure data transfers, for example by using the encrypted HTTPS protocol in the web environment. Controlling users' access to systems and resources is also crucial to guarantee confidentiality. Pseudonymization and anonymization are also suggested by GDPR and PDPA as concrete security measures to mitigate the risk of identifying a specific individual and boost confidentiality and user privacy. In addition to ensuring confidentiality, encryption and access controls are also ways to guarantee *integrity*. Integrity – discussed in GDPR, PDPA, DPA, SCD and ETA – guarantees that data is correct and reliable and not altered in an unauthorized manner [25]. Finally, GDPR and PDPA also talk about *availability*. Mostly distinct from the concept of privacy, availability means ensuring the data is accessible when needed.

Authentication, verifying the identity of a user, is also a key concept for protecting users' privacy in GDPR, PDPA, CSD and ETA. At implementation level, this involves different authentication mechanisms such as multifactor authentication (CSD). Along with authentication, *authorization* is mentioned in GDPR, PDPA and CSD. Authorization – ensuring that users only have access to resources they are permitted to use – is ensured at implementation level with access control mechanisms (PDPA and DPA).

GDPR emphasizes several kinds of *user autonomy* [2]. This includes the rights to, for instance, object to data processing, access their personal data, and correct inaccuracies in the data These same rights are also protected by PDPA. A website collecting data, for example, should include clear instructions on how to exercise these rights and possibly contain features such as forms to make requests pertaining to their stored personal data. To respond to such requests, organizations must also maintain records of data processing activities. Likewise, the user's *free consent* and the right to withdraw it at any time are important parts of the GDPR. In the web environment, this usually means consent banners as an implementation level solution. These banners should give the user clear options to accept or reject data processing, without any deceptive design practices or dark patterns such as pre-ticked consent boxes or absence of the reject button. While PDPA seems to imply that consent should be "freely given", the GDPR is much more expressive in this respect – it requires that the user grants freely given, specific, informed, unambiguous, and explicit consent.

GDPR and PDPA stress *data minimization* [4]. Minimizing collected data, having a small number of third party data processors, and having clear data retention periods all serve this purpose in implementation. The possibility to decline or reduce data collection, discussed previously, also contributes to data minimization. Data transfers should also be minimized and *secure data processing* should be guaranteed. This is especially true for data transfers outside the EU or EEA (in GDPR) or data transfers outside Sri Lanka (in PDPA). In other words, ensuring secure cross-border data transfers and sufficient protection mechanisms are essential when transferring data outside these jurisdictions. The GDPR and PDPA also discuss "special category data", sensitive personal data on health, political opinion, race or ethnicity, religious beliefs, etc. These categories require special protection and secure processing.

According to the GDPR and PDPA, the data controllers have the obligation of *informing the user adequately* of the data processing activities. In practice, this means that the user has to be provided with *clear and transparent privacy statements*, usually in the form of privacy policy documents.

Other concepts mentioned in the regulations are resilience (DPA) and cyber hygiene (CSD). Unfortunately, the practical ways to enforce these ideas in software development are left unclear. To be *resilient* against cyberattacks a software system or a website has to employ several cybersecurity and privacy measures such as regular backups, updates, encryption, etc. The ability to respond to privacy incidents is also part of resilience. For example, the GDPR states that organizations have an obligation to notify the data protection authority of personal data breaches soon after they become aware of such incidents. Therefore, in practice, some kind of a technical data breach detection mechanism is needed. Similarly, *cyber hygiene* is a very general term for practices that organizations can take to keep their systems healthy and protect sensitive data from different threats. These include for example regular updates, requiring strong passwords, malware protection etc. [28]

It is clear from this examination that most of the concepts and practical privacy measures discussed here stem from the GDPR and PDPA, and these acts form the backbone of privacy regulation in their respective areas. The two acts essentially provide the same practical requirements for the software developers. Based on the previous conceptual analysis, we chose to examine the following characteristics on the selected websites:

- *Use of HTTPS*. This guarantees the confidentiality and integrity of data during transmission.
- *Presence of a cookie consent banner* or other clear method to ask for consent for cookies and data collection. A valid cookie consent banner implements the freely given consent required by PDPA and GDPR.
- *Presence of privacy policy* or other form of document adequately informing the user of data processing activities, required by GDPR and PDPA.
- *Readability of privacy policies*. The policies were assessed using the Flesch-Kincaid readability test [23].

- *The number of third parties receiving personal data.* Data transmissions to third parties without consent can be problematic in terms of GDPR and PDPA. Also, excessive number of third-party connections transferring personal data goes against the data minimization requirement of both GDPR and PDPA.
- *Cross-border data transmissions.* In the EU, according to GDPR, data transfers outside the EU or EEA may be problematic for example if the user is adequately informed or they have not consented to the transfer. Similarly, in Sri Lankan PDPA gives the same conditions for cross-border data transfers.
- *Dark patterns* In this study, we investigated the use of three different dark patterns in cookie consent banners. The dark patterns we studied were the absence of a rejection button in the first layer of the banner, use of pre-ticked consent boxes and the use of deceptive colors and contrasts. These patterns are defined in the European Data Protection Boards Cookie Banner Taskforce's "Report of the work undertaken"[3], and have been chosen because their presence is effortless and straightforward to determine in most cases.
- *Availability* of the service.

Naturally, the choice to examine these specific aspects and features is not exhaustive, and privacy issues and compliance issues cannot even comprehensively be studied just by looking at a website's public-facing client side. However, we believe these selected characteristics still give a good and clear picture of how well real-life websites comply with the existing privacy regulation. It is also worth noting that since GDPR and PDPA, in the end, require very similar practical privacy measures for compliance, the criteria we used to assess Finnish and Sri Lankan websites are the same.

4.2 Empirical Survey of Websites

4.2.1 Finnish Websites. Out of the 63 Finnish governmental websites, majority fared quite well in our survey. 7 out of 63 (11.1%) of them did not have cookie consent banners, and additional 4 had only a "visitor tracking banner", which prompted the user to turn off cookie usage from browser settings. This form of declining tracking is not considered as a valid way of consenting to data collection and does not comply with the GDPR. It must also be noted that 3 of the websites that did not have the cookie consent banner did engage in collection of user data, which is a very questionable practice. Out of the 63 Finnish government websites, 9 (12.7%) had deceptive colors and contrasts in their cookie consent banners. One (1) government website had pre-ticked boxes in its cookie consent banner, which is a violation of the GDPR. All of the 63 Finnish governmental websites were available and all used HTTPS.

The government websites had only 0.27 third parties per website, receiving personal data such as visited websites and search terms combined with identifying information like IP address. 84.1% of the websites had no third parties receiving this kind of problematic personal data. However, taking into account we did not give consent for cookies or any data collection, these numbers could still be smaller. The third parties receiving personal data from Finnish public sector websites are shown in Figure 1. Snoobi, a privacy oriented analytics service based in Finland, is he largest data collector, which shows public sector cares about privacy and aims to keep collected data in Finland. However, tech giants like Google, Microsoft and Meta are also present, receiving personal data such as receiving data on the user's page visits, and possible involving cross-border data transfers. It is worth noting that this all happened without consent.

Moreover, 12 of the 63 websites (19.0%) did not have a proper privacy policy document. Some of these has "cookie policies" which are also considered as privacy policies here. When it comes to readability, 8 of the 51 websites (15.7%) that had the privacy policy had a policy that was deemed "Very hard to read", requiring at least college graduate level education to comprehend, while the rest of the websites had merely "Difficult to read" policy, which was deemed understandable with entry-level college education. To put this in perspective, it should be noted that in Finland the high school equivalent education is pursued by roughly 54% of the respective age class yearly[4], while college level education is possessed by roughly 41% of the total adult population[5].

Of the 15 Finnish private sector websites we studied, almost all fared very well in the study in all of the inspected categories. All websites had a privacy policy among which 2 had a privacy disclaimer. One of these was very short and thus insufficiently explained how the user data was handled. The Finnish companies had no dark patterns in their cookie consent banners other than deceptive colors and contrasts coaxing the user into selecting the "Accept" button in 12 out of 15 cases (80%). The recipients of personal data leaks on Finnish company websites are shown in Figure 2. Unsurprisingly, Google is the largest data collector with 5 occurrences.

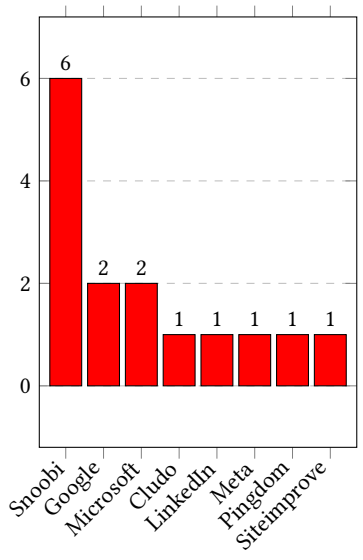


Figure 1: Data leaks in Finnish public sector.

[3]https://www.edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en

[4]https://stat.fi/til/khak/2020/khak_2020_2021-12-09_tie_001_fi.html

[5]https://yle.fi/a/3-10962640

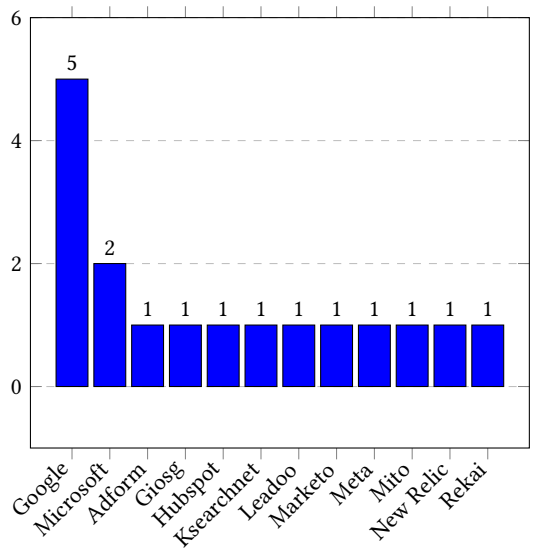


Figure 2: Data leaks in Finnish private sector.

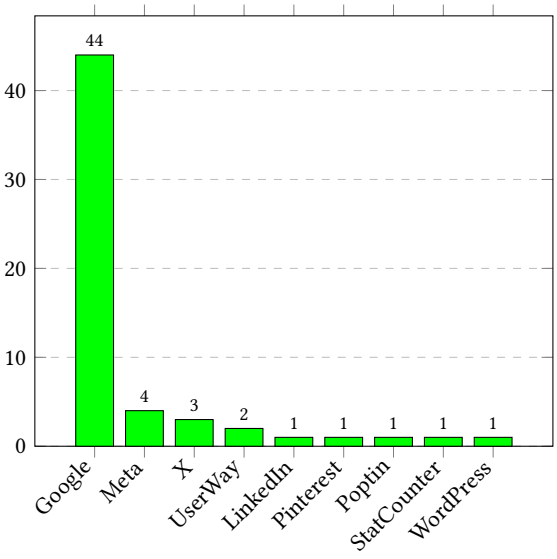


Figure 3: Data leaks in Sri Lankan public sector.

4.2.2 Sri Lankan Websites. Total number of inspected Sri Lankan governmental websites was 105, but only 94 of these websites were available and could be studied. A remarkably small number of the studied websites, only 6 of the 94 (6.4%), had a cookie consent banner. Moreover, 2 of these did not give the user a chance to decline data collection, but only offered a "Got it!" button. This does not fulfill the requirement of freely given consent. Of the websites that had cookie consent banners, three (3) had dark patterns, different on each banner. One used pre-ticked consent boxes, one had a banner that hid the rejection button to second layer of the banner and one that had deceptive colors and contrasts. The remaining three (3) websites with banners had banners that did not allow for declining cookies at all. Figure 3 shows the recipients of personal data leaks on Sri Lankan government websites. Google is overwhelmingly the largest data collector with 44 occurrences, and cross-border transfers of personal data do not seem to be a great concern. The numbers of data leaks per website, 0.62, is significantly larger than on Finnish government websites.

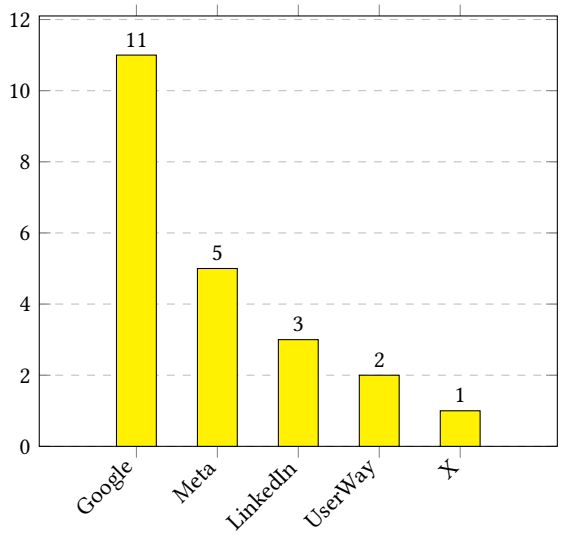


Figure 4: Data leaks in Sri Lankan private sector.

Only 11 out of 94 (11.7%) websites had a privacy policy document. This was despite the fact that informing users adequately about data processing activities is required by the PDPA. Moreover, 10 out of 94 (10.6%) did not use HTTPS. In general, the few Sri Lankan governmental websites that had privacy policies had policies that were slightly easier to read than their Finnish counterparts, with 3 (27.3%) of the policies being deemed requiring high-school equivalent education to understand, and the rest (72.7%) being comprehensible to people with entry-level college education. Although privacy policies were much less common in Sri Lankan government websites, they were also more readable as none were considered to require college graduate levels of education. However, this may also party be due to the GDPR requiring quite comprehensive (and thus easily complex) privacy policies.

Sri Lankan private sector websites fared better in our survey than the governmental institutions, but not perfectly. Only 5 out of 16 (31.25%) inspected company websites had cookie consent banners. One (1) of these websites had a banner that did not give any options for declining cookies. One (1) had a banner that did not have any dark patterns, while the remaining three (3) had a mixture of different dark patterns in use, with one of them exhibiting all three dark patterns, one pre-ticked consent boxes and deceptive colors and one only with deceptive colours. 9 out of 16 (56.25%) websites had privacy policies, although it must be noted that two of these documents only marginally fulfilled this role. All of the websites were available, and all used HTTPS. Figure 4 illustrates the third parties receiving personal data on Sri Lankan company websites. Google is very common here with 15 occurrences, which is a proportionally larger number than in the public sector. Other than

	SL gov	FI gov	SL companies	FI companies
Cookie banner	6.4%	88.9%	31.3%	100%
HTTPS	89.4%	100%	100%	100%
Privacy policy	11.7%	81.0%	62.5%	100%
Readability	46.0	38.6	39.8	41.6
No 3rd parties	49.5%	84.1%	25.0%	40.0%
Data leaks per website	0.62	0.27	1.38	1.20

Table 2: Comparison of Sri Lankan and Finnish websites.

this, however, the private sector still does better. The better result in the private sector is likely to be a sign of effective self-regulation of large companies.

Table 2 summarizes several aspects of our empirical study. We can see, for example, that cookie banners and privacy policies are used much more frequently on Finnish websites, reflecting Finland's stricter privacy regulation and more effective enforcement. Even HTTPS is not always employed on Sri Lankan websites. While the readability scores of Sri Lankan government websites' privacy policies is high, meaning the documents are readable, this is possibly also due to the fact that the documents are often simple and succinct, lacking the information necessary for the user. finally, when it comes to third parties collecting personal data, we can Finnish websites much more often have no third parties when consent is not given. Finally, Finnish websites have a lower number of data leaks per website.

5 Discussion

The key takeaway of this study has been that robust privacy regulation such as GDPR, and especially the duration the regulation has been in place, obviously has an effect on how the website maintainers take the privacy matters into account. The difference in the use of cookie consent banners and privacy policies between Sri Lankan and Finnish websites is clear, with the former mostly not having these features while the latter mostly having them, and the only observable cause for this seems to be the length of time the regulation has been in place. The numbers of third party data transfers without the user's consent are also lower on Finnish websites. GDPR was instituted over half a decade ago in 2018, and the Finnish website maintainers have had time to accommodate the mandates it imposes, such as de facto necessity of having cookie consent banners. In contrast, Sri Lanka has only quite recently introduced their own Personal Data Protection Act in 2022, which is not yet fully being enforced. Therefore, it is not surprising that its effects are not yet visible.

However, apart from this discrepancy in regulatory matters, it should be noted that there seemingly exists a cultural difference in the attitudes towards the use of web analytics between these two countries. In Finland, tools like Matomo are widely used especially in public sector. Matomo is a locally deployed web analytics tool, meaning the maintainer of the website can retain the control of collected data [19], which makes it an advisable tool when it comes to user privacy. The studied Sri Lankan websites did not use it at all, instead opting for external analytics services, which often caused data transfers outside the country. While it is debatable whether the public sector websites should be using web analytics tools in the first place, it is obvious that if such tools are used, they should not be prone to leaking data to third parties.

In principle, public sector bodies should be extremely compliant with legislation – after all, they represent the state that imposes the legislation and upholds the rule of law, and thus the representatives of the state should be exemplars in this matter [27]. While Sri Lankan institutions fared worse than their Finnish counterparts in this respect, it should be noted that the Finnish institutional websites had some problems too. Not only did some of them use the quite questionable method of transferring the responsibility of declining cookies to the user by calling for adjustment of browser settings – something that most end-users cannot be expected to handle, their cookie consent banners too often included dark patterns. While not all dark patterns and questionable privacy practices are de jure illegal, but as the saying goes "When someone has to say that nothing illegal has happened, it is obvious that whatever happened was fundamentally immoral".

Private sector websites, both in Sri Lanka and in Finland, displayed better adherence to the rule of privacy legislation than the public sector institutions. It should be noted that in the case of both countries, the companies we studied were among the largest in their respective countries, and this is likely to have something to do with the issue. Larger companies are under more scrutiny from the society at large, and have higher stakes in upholding a certain image of acting in compliance with regulations.

Lastly, it is worth noting that the ethical and ethnographic aspects can also influence laws and regulations and their enforcement. While Sri Lanka has adopted privacy regulation based on the European GDPR, it has also been shown that cultural differences can cause individuals in Sri Lanka to feel uncomfortable about Western privacy laws and practices [15]. It is important to consider how appropriate it is to conform to Western ethical rules in Asian privacy regulation and whether it is possible to achieve a truly global concept of privacy.

6 Conclusion

In this paper, we have investigated the differences between Finnish and Sri Lankan websites in privacy matters, and how the privacy regulations affect these things. Our results imply that having robust privacy regulations in place does have a positive effect by improving privacy and compliance, but it takes a certain time for the regulation to take effect. This also requires efficient enforcement of the regulation in practice. In future, it will be interesting to see how the privacy of web services changes in Sri Lanka in

the coming months when the PDPA comes into full force. A future research direction is to increase the number of studied websites, especially in private sector. Furthermore, another avenue to extend our research is to concentrate on how regulation is implemented the back end of the websites.

Acknowledgments

This research has been funded by Academy of Finland project 327397, IDA – Intimacy in Data-Driven Culture.

References

[1] Thusitha B Abeysekara and Amali E Ranasinghe. 2022. Holistic Approach in Introducing Proper Legal Framework to Regulate Data Protection and Privacy in Sri Lanka. *Journal of Business Research and Insights (former Vidyodaya Journal of Management)* 8, I (2022).

[2] Sanju Ahuja and Jyoti Kumar. 2022. Conceptualizations of user autonomy within the normative evaluation of dark patterns. *Ethics and Information Technology* 24, 4 (2022), 52.

[3] Vibhushinie Bentototahewa. 2021. *A Framework for Acceptance and Implementation of Global Data Privacy and Security Policies by States (A Case Study of Sri Lanka and United Kingdom).* Ph. D. Dissertation. Cardiff Metropolitan University.

[4] Asia J Biega, Peter Potash, Hal Daumé, Fernando Diaz, and Michèle Finck. 2020. Operationalizing the legal principle of data minimization for personalization. In *Proceedings of the 43rd international ACM SIGIR conference on research and development in information retrieval.* ACM, 399–408.

[5] Robin Carlsson, Panu Puhtila, and Sampsa Rauti. 2023. Towards an automatic tool for detecting third-party data leaks on websites. *Proceedings http://ceur-ws. org ISSN* 1613 (2023), 0073.

[6] Grazia Cecere, Fabrice Le Guel, and Nicolas Soulié. 2015. Perceived internet privacy concerns on social networks in Europe. *Technological Forecasting and Social Change* 96 (2015), 277–287.

[7] Nipuna Dissanayaka. 2020. Analysis of Sri Lankan Cyber Laws To Prevent a Cyber Warfare. *Available at SSRN 3855707* (2020).

[8] Graham Greenleaf. 2019. Advances in South Asian data privacy laws: Sri Lanka, Pakistan and Nepal. *Pakistan and Nepal (December 1, 2019)* (2019), 22–25.

[9] Timi Heino, Robin Carlsson, Sampsa Rauti, and Ville Leppänen. 2022. Assessing discrepancies between network traffic and privacy policies of public sector web services. In *Proceedings of the 17th international conference on availability, reliability and security.* ACM, 1–6.

[10] Tuija Kautto and Pekka Henttonen. 2017. Availability and findability of FOI and privacy statements on Finnish municipalities' websites. *Tidskriftet Arkiv* 8-1 (2017).

[11] Adrian Kulathunga. 2019. A Comparative Study on Sri Lankan v. European Cybercrime Law in Protecting IT Professionals and Victims of Cyber-attacks. *European Cybercrime Law in Protecting IT Professionals and Victims of Cyber-attacks (January 8, 2019)* (2019).

[12] Ponnurangam Kumaraguru and Niharika Sachdeva. 2012. Privacy in India: Attitudes and awareness v 2.0. *Available at SSRN 2188749* (2012).

[13] KK Madugalla. 2016. Right to Privacy in Cyberspace: Comparative Perspectives from Sri Lanka and other Jurisdictions. In *Kelaniya International Conference on Advances in Computing and Technology (KICACT) – 2016.* Faculty of Computing and Technology, University of Kelaniya, Sri Lanka.

[14] Justin D Martin, S Shageaa Naqvi, and Ifath Arwah. 2020. Attitudes about Censorship and Internet Surveillance among South Asians and nationals in the Arab Gulf: Predictors of digital self-expression values. *International Communication Research Journal* 55, 1 (2020).

[15] Bardia Monshi and Verena Zieglmayer. 2004. The problem of privacy in transcultural research: Reflections on an ethnographic study in Sri Lanka. *Ethics & Behavior* 14, 4 (2004), 305–312.

[16] Tavini Nanayakkara. 2024. An analysis of privacy policies in Sri Lanka. *University of Colombo Review* 5, 1 (2024).

[17] Dinuka Navaratna. 2020. Laws in Sri Lanka to Prevent Cyber-Attacks: Analysis of Laws in Sri Lanka to Prevent Cyber-Warfare in the Future. *Available at SSRN 3664868* (2020).

[18] Panu Puhtila, Timi Heino, and Sampsa Rauti. 2024. Third-Party Data Leaks and Dark Patterns in Finnish Political Websites. In *Proceedings of the International Conference on Computer Systems and Technologies 2024.* 43–50.

[19] Denise Quintel and Robert Wilson. 2020. Analytics and Privacy: Using Matomo in EBSCO's Discovery Service. *Information Technology and Libraries* 39, 3 (2020).

[20] S. Y. Rajapaksha, L. G. P. K. Guruge, and S. L. P. Yasakethu. 2023. *Emerging Computer Security Laws and Regulations Across the Globe: A Comparison Between Sri Lankan and Contemporary International Computer Acts.* Springer International Publishing, Cham, 195–215.

[21] PA Ranathunga and Ruwan Wickramarachchi. 2021. Designing a data governance model to implement GDPR in Sri Lankan enterprises. International Conference on Industrial Engineering and Operations Management, IEOM Society.

[22] Harshani Menaka Ratnayake. 2013. Negotiating privacy, confidentiality and security issues pertaining to electronic medical records in Sri Lanka: A comparative legal analysis. *Sri Lanka Journal of Bio-Medical Informatics* (2013).

[23] Marina Solnyshkina, Radif Zamaletdinov, Ludmila Gorodetskaya, and Azat Gabitov. 2017. Evaluating text complexity and Flesch-Kincaid grade level. *Journal of social studies education research* 8, 3 (2017), 238–248.

[24] Vishaka Sooriyabandara. 2016. Balancing the Conflict between Right to Information and Right to Privacy under Sri Lankan Fundamental Rights Perspective. *Sabaragamuwa University Journal* 15, 1 (2016), 1.

[25] William Stallings, Lawrie Brown, Michael D Bauer, and Michael Howard. 2012. *Computer security: principles and practice.* Vol. 2. Pearson Upper Saddle River.

[26] Anselm Strauss, Juliet Corbin, et al. 1990. *Basics of qualitative research.* Vol. 15. SAGE, Newbury Park, CA.

[27] Nik Thompson, Ravi Ravindran, and Salvatore Nicosia. 2015. Government data does not mean data governance: Lessons learned from a public sector application audit. *Government information quarterly* 32, 3 (2015), 316–322.

[28] Arun Vishwanath, Loo Seng Neo, Pamela Goh, Seyoung Lee, Majeed Khader, Gabriel Ong, and Jeffery Chin. 2020. Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems* 128 (2020), 113160.

[29] Dimitrios Zissis and Dimitrios Lekkas. 2012. Addressing cloud computing security issues. *Future Generation computer systems* 28, 3 (2012), 583–592.