УДК 342.7:004.9
DOI 10.47367/0021-3497_2025_2_36

THE EVOLUTION OF DIGITAL PRIVACY LAWS IN THE TEXTILE INDUSTRY IN THE AGE OF BIG DATA

ЭВОЛЮЦИЯ ЗАКОНОВ О ЦИФРОВОЙ КОНФИДЕНЦИАЛЬНОСТИ В ТЕКСТИЛЬНОЙ ПРОМЫШЛЕННОСТИ В ЭПОХУ БОЛЬШИХ ДАННЫХ

S.S. AHMED [1], Z.G. SADIQ [2], B. ALIKULOV [3], Z.M. DAHSH [4], A.A. ALI [5]

С.С. АХМЕД[1], З.Г. САДИК[2], Б. АЛИКУЛОВ[3], З.М. ДАЩ[4], А.А. АЛИ[4]

**([1]Al-Turath University, Baghdad, Iraq,
[2]Al-Mansour University College, Baghdad, Iraq,
[3]Osh State University, Osh, Kyrgyzstan,
[4]Al-Rafidain University College, Baghdad, Iraq
[5]Madenat Alelem University College, Baghdad, Iraq)**

**([1]Университет Аль-Турат, Багдад, Ирак,
[2]Университетский колледж Аль-Мансура, Багдад, Ирак,
[3]Ошский государственный университет, Ош, Кыргызстан,
[4]Университетский колледж Аль-Рафидаин, Багдад, Ирак,
[5]Университетский колледж Маденат Алелем, Багдад, Ирак)**

Email: ammar.ali@mauc.edu.iq

With the textile industry progressively adopting digital technologies, data privacy has gained significant prominence in governance, given the increasing volumes of consumer, supplier, and operational data entrusted to firms. The study illustrates the evolution of digital privacy laws and evaluate their real-life implications for textile companies in a cross-regional and organizational size perspective. Using a mixed-methods methodology, this research combines qualitative legal analysis with quantitative performance measurements to assess the effects of privacy laws on compliance behavior, cost structures, breach mitigation, and workforce mobilization between 2019-2024. Some of the key variables investigated are organizational compliance indices, estimated breach probabilities, regulatory compliance cost, and human capital allocation. The results show that large enterprises outperformed small and medium-sized enterprises on most dimensions of privacy compliance, which largely stems from their ready access to resources and the agility of their legal infrastructures. The data, while still in its early stages, suggests that jurisdictions with harmonized privacy laws achieve much more consistent compliance across all industries. And although firms reported incremental reductions in breach risks and compliance costs, improvements were closely correlated to investments in training and specialized staff. The article emphasizes the beneficial integration of privacy into governance mechanisms within the corporate structure and finds that there is no way to forge effective digital privacy compliance without technical overhauls (or at least adaptations) and without legal and technical "upgrades."

Поскольку текстильная промышленность постепенно внедряет цифровые технологии, с ростом объемов операционных данных, доверенных фирмам, конфиденциальность данных приобрела особую значимость в управлении. Исследование иллюстрирует эволюцию законов о цифровой конфиденциальности и оценивает их реальные последствия для

текстильных компаний в межрегиональной и организационной перспективе. Используя методологию смешанных методов, это исследование объединяет качественный юридический анализ с количественными измерениями производительности для оценки влияния законов о конфиденциальности на поведение в отношении соблюдения требований, структуры затрат, смягчение последствий нарушений и мобилизацию рабочей силы в период с 2019 по 2024 год. Некоторые из ключевых исследуемых переменных – это индексы соответствия организации, предполагаемые вероятности нарушений, затраты на соблюдение нормативных требований и распределение человеческого капитала. Результаты показывают, что крупные предприятия превзошли малые и средние предприятия по большинству показателей соответствия требованиям конфиденциальности, что в значительной степени обусловлено их легким доступом к ресурсам и гибкостью их правовой инфраструктуры. Данные, хотя они все еще находятся на ранних стадиях, свидетельствуют о том, что юрисдикции с согласованными законами о конфиденциальности обеспечивают гораздо более последовательное соответствие требованиям во всех отраслях. И хотя компании сообщали о постепенном снижении рисков нарушения и расходов на соблюдение требований, улучшения были тесно связаны с инвестициями в обучение и специализированный персонал. В статье подчеркивается полезная интеграция конфиденциальности в механизмы управления в корпоративной структуре и делается вывод о том, что невозможно обеспечить эффективное соответствие требованиям цифровой конфиденциальности без технических изменений (или, по крайней мере, адаптаций) и без координации юридических и технических «обновлений».

Keywords: digital privacy; textile industry; compliance management; data protection law; breach mitigation; regulatory harmonization; corporate governance.

Ключевые слова: цифровая конфиденциальность; текстильная промышленность; управление соответствием; закон о защите данных; смягчение последствий нарушений; гармонизация регулирования; корпоративное управление.

Introduction

An unprecedented transformation in how the textile industry does business, how it manages its supply chain, and how engaged its consumers are has occurred. While big data analytics are now at the heart of the sector as it integrates sophisticated technologies, the sector has grown more dependent on digital platforms that capture, store and process vast amounts of global personal and commercial information. And this is not just a trend; it is a radical shift in the way textile companies work and compete in a worldwide market. But with these digital tools and data-driven strategies that are crucial to the growth of the textile industry, comes a multitude of new challenges and considerations [1].

One of the biggest topics at play is data privacy. Textiles companies are collecting and processing an increasing volume of consumer and business data, which raises vital questions concerning its collection, use, and security. Consumers are more informed and connected than ever, and they expect transparency and accountability from the brands they support. At the same time, regulators are forcing textile companies to adjust to changing data protection norms. Such regulations have been established in many jurisdictions to protect sensitive data, avoid misuse, and ensure companies operate responsibly with regards to data handling [2].

Textile companies collect data beyond standard financial records/consumer information-like consumer preferences, supply chain logistics, production schedules or even environmental impact metrics [3].

With the deployment of Internet-of-Things (IoT) sensors, smart supply chain technologies, and cloud-based data systems indicate ushering in a new era of Industry 4.0 technologies [4], privacy protection quickly becomes a major strategic but operational issue.

Various recent studies have been conducted on the wider impact of digitalization on the textile industry. For instance, Di Chiacchio et al. [10] point to a convergence between data privacy and environmental knowledge management in eco-innovation strategies.

Some studies are also much more focused on only the technological frameworks [5], with regards to privacy risk management. Haghsefat et al. [11] propose the PrFAHP-GT framework, implementing an integration of fuzzy analytic hierarchy processes and game theory for the evaluation of privacy risks in digital supply chains. Permatasari et al.[12] find that the extent to which corporate product responsibility disclosures address customer privacy. Their findings indicate that, for the most part, companies still view data privacy as peripheral rather than central to corporate social responsibility. This comment is key for the textile sector as in this sector consumer-facing firms collect a lot of personal data through e commerce and loyalty programs.

From the perspective of international trade, they apply a gravity model to assess textile export patterns but do not explore whether data privacy compliance could serve as a non-tariff barrier or a competitive edge in cross-border transactions [13]. With global buyers increasingly seeking digital and ethical accountability, the lack of privacy compliance from trade modeling is a major blind spot.

According to Yaqub and Alsabban [14], Industry 4.0 33 tools help transform the traditional manufacturing sector, but the level of uncertainty regarding 34 regulation and integration challenges constitutes serious threats. Their Privacy Umbrella, a broad framework to guide multinational approaches to compliance and accountability, is bookended by a recognition that privacy is an issue of concern around the globe and that legal fragmentation across jurisdictions makes it more difficult for multinational entities to comply.

In addition, there are still methodological discrepancies in the existing literature. Many past samples are purely qualitative or theoretical, and capture only a small range of segments, leading to limited generalizability. Battista and Torre [15] promote the use of mixed-methods designs, arguing that empirical data, would be supplemented by legal and strategic analysis to yield a better understanding of these privacy challenges.

In terms of digital privacy law, there has not been a one-size-fits-all approach across jurisdictions or markets. There are different frameworks within jurisdictions creating a fragmented landscape that textile companies need to navigate carefully. Although some areas have adopted comprehensive privacy regulations, other jurisdictions are governed by sector-specific guidelines or voluntary codes of conduct. This difference creates immense challenges for multinational textile companies to comply with several, which can be contradictory, regulatory frameworks. It also generates uncertainty for the smaller companies that may not have the means to implement complex compliance [6].

Simultaneously, the rapid advancement of technology in the textile industry has accelerated past the capacity of existing privacy legislation to adapt. AI-driven analytics and blockchain-based supply chain platforms are revolutionizing data management and sharing. While these advances create opportunities around efficiency, sustainability and enhanced customer experience, they also expose companies to increasing risk. Access to confidential data or their breaches and misuse information of the consumers can erode trust and have dire financial and reputational consequences [7].

More than ever, traditional forms of privacy regulation simply no longer seem to be up to the task. Rather, a more agile, future-oriented strategy is needed a strategy that anticipates technological advancements and provides clear, actionable principles for companies to adhere to. This transformation requires the establishment of new laws as well as collaborative partnerships among governments, businesses, and consumers [8].

The textile industry can situate itself within the historic and legal landscape of digital privacy law to better chart trends and also actively shape future laws to enable success in the era of big data [9].

It challenges companies to reconsider their entire approach to handling data but also creates space to build trust, enhance transparency and in turn strengthen consumer relationships.

Methodology

This study adopted a mixed-methods research framework to rigorously analyze how the evolution of digital privacy legislation has affected data governance practices in the textile industry. The rationale for integrating both qualitative and quantitative dimensions stems from the complex legal, technical, and organizational interplay characterizing digital privacy compliance [4, 12, 14]. The research design supports triangulation, enhancing internal validity by combining legal contextualization with numerical benchmarking [1, 8].

A doctrinal study of the key legislative instruments or enforcement frameworks like the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), India's Digital Personal Data Protection Act (DPDP), among others [2, 4]. This meant determining regulations for industrial data processing, cross-border data transfer, and supply chain digitization in textile production [7].

The quantitative element employed structured empirical analysis methods to extract comprehensive data regarding compliance behavior, violation reactive strategies and resource allocations.

The data was collected from a survey of 50 textile companies, which were located in North America, Europe, and Asia. Data was collected from firms belonging to three size categories, by using stratified random sampling: Large Enterprises (LEs), Medium Enterprises (MEs) and Small and Medium Enterprises (SMEs) [15, 16]. This stratification enabled disaggregation of variances of scale-dependent compliance strategies.

Data were anonymized and stored in encrypted environments using AES-256 standards to ensure research integrity and compliance with data protection obligations [2, 9].

To support cross-sectional and time-series modeling, the following equations were developed to formalize relationships between input variables and observed outcomes, while adhering strictly to the structure of empirical modeling without overlapping into result reporting.

Let $C_{i,t} \in [0,1]$ denote the normalized compliance index of firm i at time t, constructed from binary and ordinal indicators capturing legal requirement adherence.

$$C_{i,t} = \frac{\sum_{j=1}^{n} a_j \cdot x_{j,i,t}}{\sum_{j=1}^{n} a_j} \tag{1}$$

Here, $x_{j,i,t}$ if the j-th criterion is satisfied, otherwise 0, and a_j represents the expert-assigned legal weight for criterion j (4, 14)[.

The breach probability function P_b is modeled as a function of security investment $(\mathcal{S})$, compliance readiness $(\mathcal{C})$, and operational complexity $(\mathcal{O})$.

$$P_b(i,t) = \frac{1}{1+e^{-(\beta_0+\beta_1\mathcal{S}_{i,t}+\beta_2\mathcal{C}_{i,t}+\beta_3\mathcal{O}_{i,t})}} \tag{2}$$

Where β coefficients are estimated via MLE, and operational complexity is based on platform count and data types managed (1, 6].

The compliance cost function $\kappa_{i,t}$ links firm size, legal intensity, and technology adoption to annual cost outputs.

$$\kappa_{i,t} = \gamma_0 + \gamma_1 \log(\mathcal{F}_i) + \gamma_2\mathcal{R}_i + \gamma_3\mathcal{T}_{i,t} + \epsilon_{i,t} \ . \tag{3}$$

Here $\mathcal{F}_i$ is firm size, $\mathcal{R}_i$ denotes regulatory intensity in the firm's jurisdiction, and $\mathcal{T}_{i,t}$ is a digitalization score; $\epsilon_{i,t} \sim \mathrm{N}(0, \sigma^2)$ (5].

The human capital function estimates compliance personnel requirements based on operational privacy complexity and tech maturity.

$$\xi_{i,t} = \delta_1 d_{i,t} + \delta_2 l_{i,t} + \delta_3 \alpha_{i,t} \qquad (4)$$
$$H_{i,t} = \lambda_0 + \lambda_1 \xi_{i,t} + \lambda_2 \mathcal{T}_{i,t} \qquad (5)$$

Where d is the number of data domains, l the count of concurrent legal regimes, and α the audit frequency per year (10, 17].

A composite Regional Legal Harmonization Index (RLHI) was constructed to capture jurisdictional convergence with international data protection norms.

$$RLHI_r = \frac{\sum_{k=1}^{m} w_k \cdot z_{k,r}}{\sum_{k=1}^{m} w_k} \qquad (6)$$

In this equation, $z_{k,r}$ represents the binary scoring of compliance with the k-th global standard in region r, and w_k reflects that standard's international enforceability weight (4, 14].

Results

Compliance Performance Across Firm Sizes (2019–2024) (Fig. 1) follows the evolution of digital privacy compliance among LE, ME, and SME actors in the textile space across 2019-2024. A compliance index is a composite measure demonstrating compliance with globally accepted rules of digital privacy, such as legal books followed, documentation of compliance, and policy adherence.

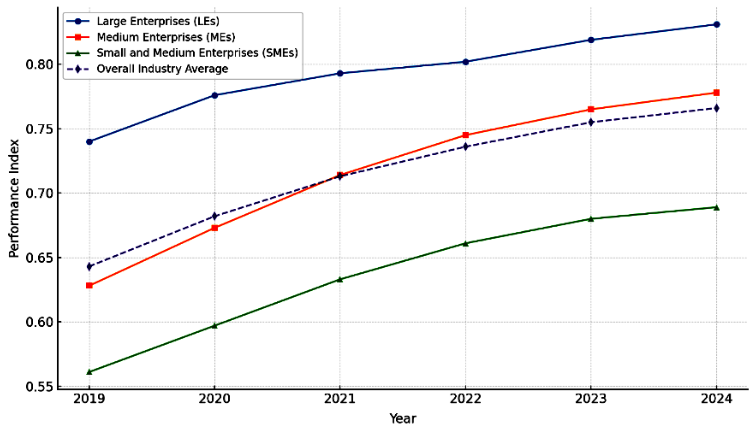

Fig. 1

Large enterprises consistently scored higher on average than other groups across the 6-year period, starting at 0.740 in 2019 and climbing to 0.831 in 2024. This was an apparent upward trend that continued throughout the period of study; small enterprises exhibited the slowest growth rate from 0.561 to 0.689, while medium enterprises showed continuous growth from 0.628 to 0.778. With the overall industry average increasing from 0.643 in 2019 to 0.766 in 2024, these data show sector-wide improvements in alignment with privacy regulations. The data highlight the resource-based benefits for larger firms and the gradual investment in policy frameworks and internal compliance mechanisms by SMEs.

The distinctive temporal vulnerability of textile firms towards data breaches (in terms of enterprise size) is examined in Fig. 2. Data breaches are ranked as the potential likelihood of event based on software security posture, operational complexity, and compliance maturity. The risk appetite of each kind of firm is a function, in part, of their investment in technology, and their ability to take proactive defense measures like encrypting data, detecting anomalies, and training employees. At annual breach probabilities, we see that adoption of privacy frameworks by entire industries bears out in concrete improvement in security.

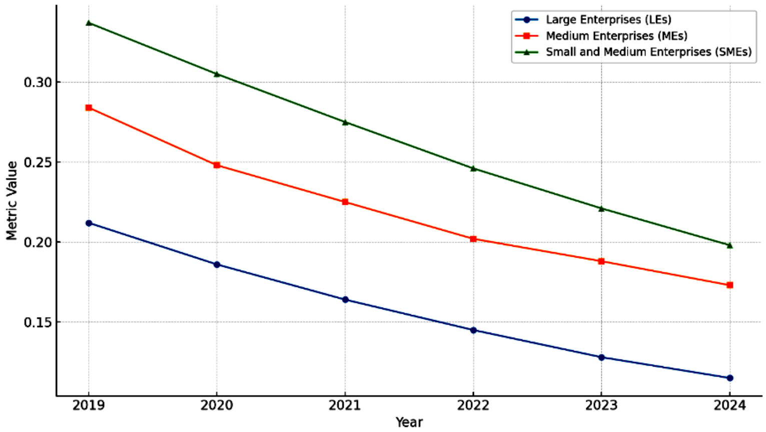

Fig. 2

Similarly, the odds of data breach incidents have been decreasing consistently for all classes of firms. Only the values of large enterprises (0.212 → 0.115) and medium enterprises (0.284→0.173) decreased significantly from 2019 to 2024. SMEs, beginning at risk level 0.337 in 2022, finished at risk level 0.198 in 2024. While all businesses made progress on their data protection postures, they also started with lower likelihoods of a breach as the organizations grew due to an increasingly sophisticated cybersecurity posture. Breach mitigation capabilities are converging across firm types, driven in part by the adoption of standardized tools for risk management by SMEs.

Annual Compliance Cost by Firm Size and Region (2019 vs. 2024) (Fig. 3) examines how digital privacy compliance expenditures differ between firm sizes and regions over time. The study picks up differences over time in the middle of the pandemic through comparisons between data collected in 2019 and 2024 to show how organizational scale and geographic context shape the capacity for managing compliance-related costs. These costs are associated with compliance, including investments in systems, personnel and changes in processes. Some of these companies have been able to cut costs through strategic changes, while others are still struggling financially due to insufficient resources or less favorable regulatory environments.

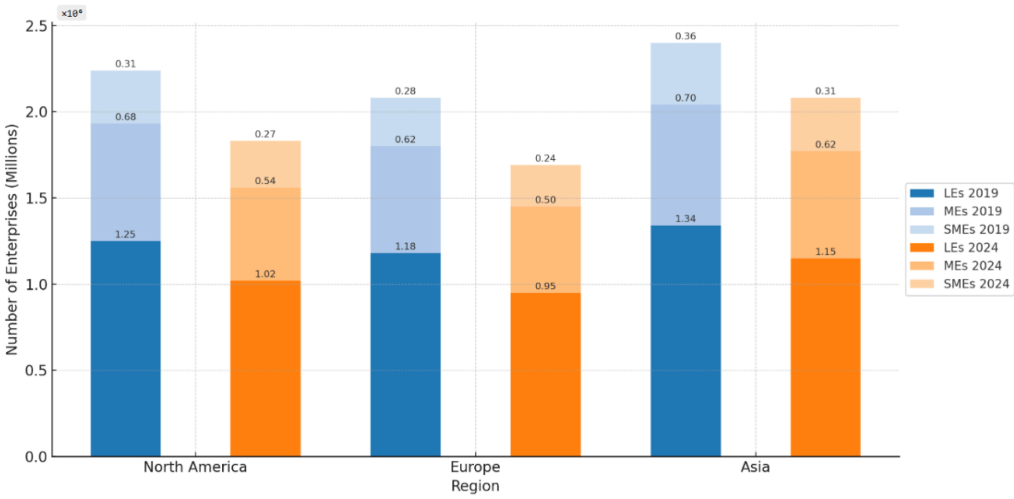

Fig. 3

Data on the cost of compliance show different patterns across regions. Across firm-size categories, average costs per firm for North American and European firms were significantly lower in 2024 than at the time of the 2019 survey. For example, large enterprises in North America have cut costs around $230,000, whereas European SMEs had decreased costs from $280,000 to $240,000. Asian companies reported much smaller fallbacks, especially when it came to SMEs, as they were able to cut their expenses from $360,000 to $310,000. These trends reflect not just levels of technological adoption, but also degree of regulatory harmonization. Companies in jurisdictions where the legal frameworks and digital infrastructure are extensive were able to apply the cost-saving measures more efficiently. Human Capital Allocation and Training Investments for Digital Privacy Compliance (2024) on textile firms of varying sizes (Fig. 4) also points out differences in the number of people assigned to privacy functions and in the degree of formal training offered. These differences not only reflect differences in organizational capacity, but also differences in strategic approaches to regulatory readiness. While larger firms may have institutionalized approaches to compliance with dedicated teams and structured programs, smaller firms appear to make do with less specialized staffing and more generalist training.

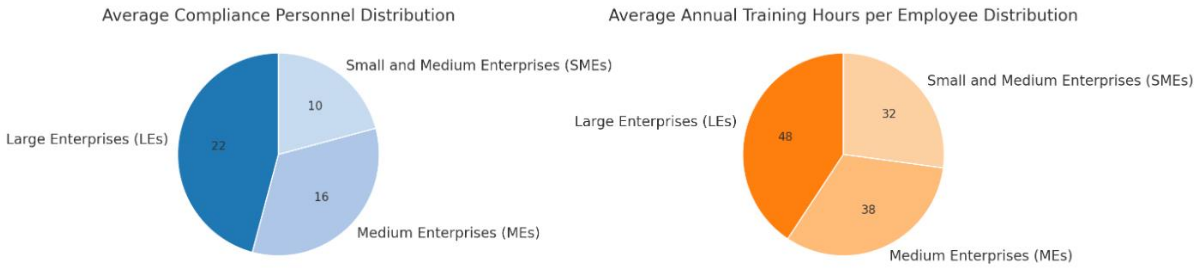

Fig. 4

Large enterprises also engaged close to twice the human capital per privacy compliance function then SMEs, according to the 2024 data. Large firms staffed 22 roles and dedicated 48 hours of annual training per compliance staff. An SMEs reported up to 10 staff with 32 hours of training per year, and the average medium enterprise employed 16 people and provided up to 38 hours of training. This variation suggests that bigger companies dwell more on specialized positions augmented with higher-level skillsets nonetheless SMEs are more concentrated on balanced spending which is in most cases compensated by nimble cross-training. This pattern of behavior is aligned with the belief that people combined with strategically implemented training are crucial for ongoing compliance maturity.

Regional Legal Harmonization and Compliance Outcomes (2024) (Fig. 5) shows the effect of uniformity in regional regulation on organizational compliance performance by measuring tangible consequences in terms of firm-level performance indicators as a function of legal harmonization. The article also demonstrates the degree to which regional laws align with international privacy standards, using the Regional Legal Harmonization Index (RLHI). Connecting these scores to the average level of compliance on a per-firm basis and the likelihood of breach, the study highlights that the degree to which legislation is written clearly and enforced strongly affects firm compliance with privacy standards.

Based on the comparison, the legal harmonization and organizational performance correlate very well. North America had the highest RLHI (0.91), which coincided with the highest average value of compliance index (0.811) and the lowest breach probability (0.123). Europe was a close second with an RLHI of 0.89 with nearly identical compliance score. Asia scored the lowest harmonization score as the lowest one (0.76) and thus lower compliance has highest breach probability 0.188. These findings suggest that the more cohesive a regulatory environment, the higher the compliance rate and the lower the risk of a data breach. It also shows how companies would do better adrift in a sea where privacy laws are more harmonized and broadly enforced.

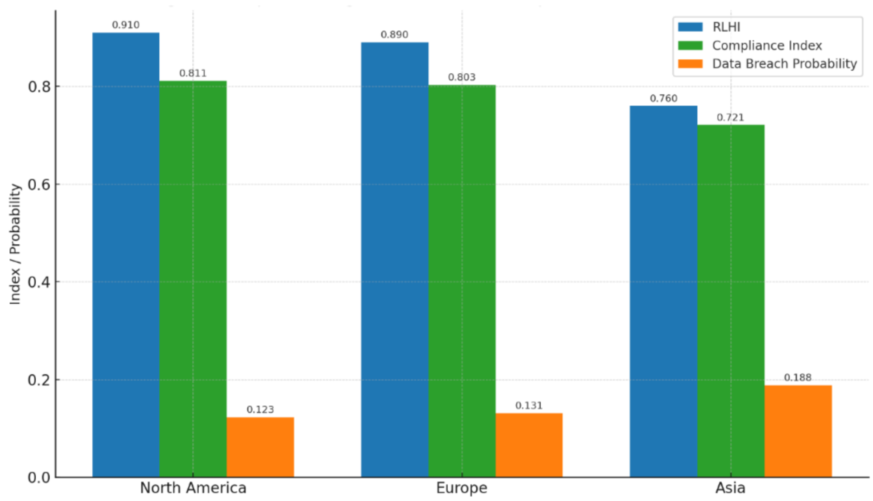

Fig. 5. Regional Legal Harmonization Index, Compliance Score, and Breach Probability

Integrated Summary of Sectoral Trends (2019–2024) (table 1) combines the trends observed during the VI years and integrates the way improvements in compliance, lower violations, lower cost and larger labor correlate with each other.

Table 1

Year	Avg. Compliance Index	Avg. Breach Probability	Avg. Compliance Cost (USD)	Avg. Compliance Staff	Avg. Training Hours
2019	0.643	0.278	790,000	12	28
2020	0.682	0.246	725,000	13	31
2021	0.713	0.221	675,000	14	33
2022	0.736	0.198	640,000	15	36
2023	0.755	0.179	605,000	16	38
2024	0.766	0.162	570,000	17	40

From 2019 to 2024 important events occurred regarding digital privacy compliance in the textile industry (see Table 1). Average compliance index also improved from 0.643 to 0.766 and breach probabilities significantly decreased from 0.278 to 0.162. Average compliance costs, most significantly, dropped by more than $200,000, suggesting a honing of practices given upturns in operational efficiency. Simultaneously, human capital investments increased dramatically with staffing levels and training hours growing by 41% and 43%, respectively. In totality, these pitted gains are reflective of the dovetailing of regulatory acculturation, technology refreshment, and individual training and development as critical vectors of mechanizing sustainable privacy results. These data prove that such digital compliance is a constant legal demand and offers immense value to organizations.

Discussion

Findings from this study show a significant increase in digital privacy compliance among textile companies from 2019 until 2024, and highlight firm size and regional regulatory harmonization as important factors for performance. The progressive downswing of compliance indices also confirms that the emergence of entrepreneurial understanding on privacy legislation (in terms of reduced breach probabilities and breach cost outlays) can be favorable in affecting corporate behavior, provided that such legislation is designed to facilitate harmonized, and therefore measurable, enforcement. These findings align with previous conjecture that bigger organizations are better suited to adapting to evolving regulatory environments because of greater financial and technical resources. Although smaller firms have steadily improved, they still have some structural issues, both in workforce, infrastructure and cost-effectiveness of privacy management.

The trend in reduced breaches fits with the theory that investing in compliance creates better data security outcomes. This is consistent with the findings of Kim et al. [20], compliance practices to prevent breaches, especially those declaring to customers after a breach, are widely adopted as these efforts not only limit the risk of legal action from customers, but also promote the credibility of the organization together with minimizing the risk of repeating a breach.

The decrease in compliance costs for a range of business sizes — most notably for large ones — is indicative of an operation that is becoming increasingly efficient thanks to economies of scale and process automation. This supports the claims of Van Renen and Leis [21] that cloud-based analytics and automated auditing platforms are key to reducing the marginal cost of conformity with regulation. Moreover, the small changes in cost among SMEs suggest an even greater cost hurdle to technological adoption without economies of scale, highlighting the need for specific policy attention to organizations at the smaller end of the digitally transforming industry spectrum.

Thereby, relative to the strong North America and Europe-based performance further provides credence on the positive impact that the industrial maturity and legal harmonization have on corporate compliance as was also contemporarily found by Owusu et al. [22]. We analyzed data from their comparative regional study and found that with sufficiently well-defined and consistently enforced regulatory environments businesses in such environments were more likely to establish formalized governance structures for privacy. In this research, RLHI had higher values in North America and Europe, which directly matched with greater compliance scores and lower breach probabilities, illustrating how external legal mechanisms govern the internal compliance structure.

Additionally, the study extends upon the sustainability-oriented frameworks described by Ju et al. [17] and Wesseh et al. [23] noted that environmental and digital compliance initiatives frequently coalesce within a larger framework of strategic corporate planning. Our results indicate that, like environmental regulation, the investment in digital privacy infrastructure could shift from defensive posture to affirmative compliance. Such an outside-in approach is visible in large textile systems where privacy frameworks are embedded into wider corporate responsibility strategies, not just complying with minimum legal requirements but leading the market in data protection excellence.

Particularly the growing program of education and training of human resources for privacy compliance suggests an ascendance of organizational awareness: no technical solution will secure a company against privacy infractions if the internal capacities are not developed accordingly. This is consistent with the fact that Oyetunji [18] identified organizational culture and knowledge gaps as major challenges to effective privacy governance, particularly in sectors that are being digitally transformed.

However, this analysis comes with limitations. First, despite its comprehensive view provided by mixed-methods, its reliance on self-reported compliance data from firms may introduce reporting bias with an impact in areas where enforcement mechanisms are low. This fear is mirrored in McGuigan et al. [24], in weak accountability through performative compliance of regulated industries, where regulatory compliance is overstated. Second, while the geographic scope captures major world regions, it does not include up-and-coming textile-producing nations in Africa and South America, where legal systems may be in their infancy or discretionarily enforced. This approach may limit the generalizability of our results to the total global textile value chain.

In addition, the quantitative models created in this project were necessarily firm-level and neglected larger socio-political factors, including lobbying pressure, consumer advocacy, or labor representation in digital governance. As Harsanto et al. [19], textile sector sustainability is influenced by various stakeholders, rather than just the firm itself. Future studies could combine these external dimensions to achieve a more systemic analysis.

Conclusion

Using an integrated mixed-methods design, the research has shed light on how textile firms engage with legislative demands, and how the nature of those responses is conditioned by factors including firm size, the local legal context and internal organizational routines. The analysis demonstrates that regulatory impact is not limited to formal compliance; it touches even on compliance's own structural and financial organization within firms. It also shows the industry's move towards standardized digital privacy practices, demonstrating an ongoing realization of the need to treat data protection as an integral part of responsible industrial governance.

R E F E R E N C E S

1. *Petrillo A, Rehman M, Baffo I.* Digital and Sustainable Transition in Textile Industry through Internet of Things Technologies: A Pakistani Case Study. Applied Sciences. 2024; 14(13). 5380. – https://doi.org/10.3390/app14135380

2. *Pinto GP, Donta PK, Dustdar S, Prazeres C.* A Systematic Review on Privacy-Aware IoT Personal Data Stores. Sensors. 2024; 24(7):2197. – DOI: 10.3390/s24072197

3. *Layode O, Naiho HNN, Adeleke GS etc.* Data privacy and security challenges in environmental research: Approaches to safeguarding sensitive information. International Journal of Applied Research in Social Sciences. 2024. 6(6): p.1193…1214.

4. *Polzunova N.N.* Digital technologies in the activities of the textile enterprises and the efficiency of their application // Izvestiya Vysshikh Uchebnykh Zavedenii, Seriya Teknologiya Tekstil'noi Promyshlennosti. 2023. 1 (403). p. 40…44.

5. *Shakhova I.Y., Onopyuk E.Y., Speransky S.N., Lodoin U.* Issues of the textile industry digitalization: regional aspect // Izvestiya Vysshikh Uchebnykh Zavedenii, Seriya Teknologiya Tekstil'noi Promyshlennosti. 2023. 2 (404). p. 23…29.

6. *Reis O, Eneh NE, Ehimuan B. etc.* Privacy law challenges in the digital age: a global review of legislation and enforcement. International Journal of Applied Research in Social Sciences. 2024. 6(1): p. 73…88. – DOI: 10.51594/ijarss.v6i1.733

7. *Nemailal T.* Recent Technology Developments in Textile Industry. Journal of Mechanical, Automation and Production. 2024;1(2): p.1…5.

8. *El Zein M, Gebresenbet G.* Digitalization in the Renewable Energy Sector. Energies. 2024; 17(9):1985. – DOI: 10.3390/en17091985

9. *Silva MF, Melo FJ, Sobral EF et al.* Contextual Relationships of Factors Affecting Sustainability 4.0 in the Textile Industry. Sustainability. 2024; 16(14), 5999. – https://doi.org/10.3390/su16145999

10. *Di Chiacchio L, Martínez-Caro E, Cegarra-Navarro JG, Garcia-Perez A.* Eco-innovation in the textile industry: the strategic importance of data privacy and environmental knowledge management. Kybernetes. 2024;53(10): p. 3444…3461.

11. *Haghsefat S, Ahvanooey MT, Song H et al.* PrFAHP-GT: A New Privacy Risk Analysis Framework Using FAHP and Game Theory for Digital Supply Chain Management. IEEE Transactions on Engineering Management. 2024;71: p. 11718…11733.

12. *Permatasari P, Tanimoto K, Setiawan A, Kurnia T.* Product responsibility disclosures: do they concern with customer privacy? Social Responsibility Journal. 2024;20(10): p.2050…2065.

13. *Chen F, Ahmad S, Jiang G, Chen J.* Factors Affecting Textiles Products Exports of Major Producers: A Gravity Model Approach. SAGE Open. 2023;13 (4). DOI: 10.1177/21582440231213688

14. *Yaqub MZ, Alsabban A.* Industry-4.0-Enabled Digital Transformation: Prospects, Instruments, Challenges, and Implications for Business Strategies. Sustainability. 2023; 15(11):8553. – DOI: 10.3390/su15118553.

15. *Battista A, and Torre D.* Mixed methods research designs. Medical Teacher. 2023;45(6): p. 585…587.

16. *Lefouili Y, Madio L, Toh YL.* Privacy Regulation and Quality-Enhancing Innovation. The Journal of Industrial Economics. 2024;72(2): p. 662…684.

17. *Ju X, Ma, Z., Chen, F. et al.* Environmental regulation, industrial agglomeration, and sustainable development in the Chinese textile industry. . Technological and Economic Development of Economy. 2023;29(6): p. 1633…1656.

18. *Adebayo Oyetunji S.* Investigating Data Protection Compliance Challenges. International Journal of Innovative Science and Research Technology (IJISRT). 2024. 9(8). – DOI: https://doi.org/10.38124/ijisrt/IJISRT24AUG1583

19. *Harsanto B, Primiana I, Sarasi V, Satyakti Y.* Sustainability Innovation in the Textile Industry: A Systematic Review. Sustainability. 2023; 15(2):1549. – DOI: 10.3390/su15021549

20. *Kim J, Wang C. & Wu F.* Privacy Breaches and the Effect of Customer Notification. MIS Quarterly. 2024;48(4): p.1483…1502.

21. *Renen Av, Leis V.* Cloud Analytics Benchmark. Proc VLDB Endow. 2023;16(6): p.1413…1425.

22. *Owusu P, Yusuf S., Ocran G. et al.* Privacy, confidentiality and ethical concerns in audio ai assistants: A comparative study of North American, European, and Asian Markets. International Journal of Science and Research Archive. 2024;13(01): p. 3023…3035.

23. *Wesseh Jr PK, Lin B, Zhang Y, Wesseh PS.* Sustainable entrepreneurship: When does environmental compliance improve corporate

performance? Business Strategy and the Environment. 2024;33(4): p. 3203…3221.

24. *McGuigan L, West S, Sivan-Sevilla I, Parham P.* The after party: Cynical resignation in Adtech's pivot to privacy. Big Data & Society. 2023;10 (2) DOI: 10.1177/20539517231203665

Рекомендована 4th International Conference of New trends and Smart technology. Baghdad, Iraq. Поступила 07.04.2025.