International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Cross-border data privacy: analyzing the united states' strategic response to GDPR compliance requirements

Adeola Okesiji [1, *], Abayomi Ogayemi [2], Odunayo Oyasiji [1], Ayotunde Omosule [2] and Adegbola Oluwole Ogedengbe [3]

[1] *Independent Researcher, Calgary, Canada.*
[2] *Independent Researcher, Toronto, Canada.*
[3] *Independent Researcher, Edmonton, Canada.*

International Journal of Science and Research Archive, 2023, 09(02), 1111-1121

Publication history: Received on 20 July 2023; revised on 23 August 2023; accepted on 28 August 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.9.2.0495

Abstract

This study examines the multifaceted approach undertaken by United States-based organizations in achieving compliance with the European Union's General Data Protection Regulation (GDPR) since its enforcement in May 2018. Through empirical analysis of corporate adaptation strategies, regulatory frameworks, and cross-border data transfer mechanisms, this research reveals a complex landscape of compliance methodologies that reflect both the extraterritorial reach of EU privacy law and the distinctive characteristics of American data governance philosophy. The findings demonstrate that U.S. organizations have developed hybrid compliance models that balance European privacy requirements with American business practices, resulting in significant organizational and technological transformations across multiple industry sectors.

Keywords: Data protection; Privacy Law; General Data Protection Regulation(GDPR); Hybrid

1. Introduction

The implementation of the General Data Protection Regulation represents a watershed moment in global data privacy governance, fundamentally altering the landscape of international data protection standards. Enacted on May 25, 2018, the GDPR's extraterritorial reach has created unprecedented compliance obligations for organizations worldwide, particularly those in the United States that process personal data of European Union residents. For United States-based organizations, GDPR compliance has necessitated comprehensive reassessment of data handling practices, privacy frameworks, and cross-border data transfer protocols.

The regulation's expansive scope encompasses any organization that offers goods or services to EU data subjects or monitors their behavior, regardless of the organization's physical location. This broad territorial application has forced American companies to confront fundamental questions about data governance, privacy rights, and the intersection of European regulatory standards with American business practices and legal frameworks.

1.1. Research Problem and Significance

This thesis extract examines the strategic responses developed by American entities to navigate the complex requirements of EU privacy law while maintaining operational efficiency and competitive advantage in global markets. The research addresses a critical gap in understanding how U.S. organizations have systematically adapted their operational, technological, and governance frameworks to achieve GDPR compliance across diverse industry sectors and organizational scales.

*Corresponding author: Adeola Okesiji

The significance of this analysis extends beyond mere regulatory compliance, encompassing broader questions of digital sovereignty, extraterritorial jurisdiction, and the evolution of privacy as a fundamental right in the digital economy. The GDPR has catalyzed a global reconsideration of privacy protection standards, with American organizations serving as important case studies in cross-border regulatory adaptation. Understanding these adaptation strategies provides valuable insights for policymakers, business leaders, and scholars examining the future of international data governance.

1.2. Digital Transformation and Data Processing Complexity

As American organizations process data from European individuals through various digital touchpoints including e-commerce platforms, social media networks, cloud services, mobile applications, Internet of Things devices, and artificial intelligence systems the imperative for robust GDPR compliance mechanisms has become increasingly critical. The proliferation of digital business models, the expansion of data analytics capabilities, and the growing sophistication of consumer digital interactions have created complex data processing ecosystems that challenge traditional approaches to privacy protection.

The COVID-19 pandemic further accelerated digital transformation initiatives, creating new data processing scenarios and compliance challenges for American organizations. Remote work arrangements, digital health monitoring, contactless commerce, and virtual service delivery models have expanded the scope and complexity of cross-border data flows, intensifying the need for comprehensive GDPR compliance frameworks.

1.3. Economic and Strategic Implications

The economic implications of GDPR compliance extend far beyond direct compliance costs, influencing market access strategies, competitive positioning, and innovation priorities for American organizations. Companies that successfully navigate GDPR requirements gain enhanced access to European markets, improved customer trust, and strengthened data governance capabilities that provide competitive advantages in an increasingly privacy-conscious global marketplace.

Conversely, organizations that fail to achieve adequate compliance face significant risks, including substantial financial penalties, market access restrictions, reputational damage, and operational disruptions. The GDPR's maximum penalty framework of 4% of annual global turnover or €20 million creates compelling economic incentives for comprehensive compliance investment, particularly for large multinational corporations.

2. Literature Review and Theoretical Framework

2.1. Theoretical Foundations

The scholarly discourse surrounding GDPR's impact on non-EU entities has evolved significantly since the regulation's inception, drawing from multiple theoretical traditions in international law, regulatory theory, and organizational studies. Bradford's (2020) concept of the "Brussels Effect" provides a foundational framework for understanding how EU regulatory standards achieve global influence through market mechanisms rather than formal legal authority. This phenomenon is particularly pronounced in the context of data protection, where the GDPR's broad territorial scope and substantial penalty provisions create compelling incentives for worldwide compliance.

The Brussels Effect operates through several mechanisms: market size effects that make compliance economically rational, regulatory stringency that establishes high protection standards, institutional capacity that enables effective enforcement, and non-divisibility that makes it impractical to maintain separate compliance frameworks for different jurisdictions. These mechanisms combine to create powerful incentives for global regulatory convergence around European standards, even absent formal legal requirements.

2.2. Cross-Border Data Governance Literature

Existing research has identified several key areas of focus in U.S.-EU data protection convergence. Schwartz (2019) emphasizes the role of adequacy decisions and transfer mechanisms in facilitating transatlantic data flows, analyzing how legal frameworks for international data transfers have evolved in response to changing geopolitical and technological circumstances. The author's examination of Privacy Shield's development and subsequent invalidation provides important insights into the challenges of maintaining stable cross-border data transfer frameworks.

Hoofnagle et al. (2019) provide comprehensive analysis of GDPR's fundamental principles and their implications for global data protection practices. Their work establishes important theoretical foundations for understanding how European privacy concepts translate into practical compliance requirements for non-EU organizations. The authors' examination of consent mechanisms, legal bases for processing, and data subject rights provides critical background for understanding the operational challenges faced by American organizations.

2.3. Organizational Adaptation and Compliance Literature

Newman (2023) examines the corporate governance implications of privacy-by-design principles for American technology companies, analyzing how European regulatory requirements have influenced internal governance structures, risk management processes, and strategic decision-making frameworks. This research provides important insights into the organizational transformation aspects of GDPR compliance, particularly for technology-intensive industries.

Johnson and Rodriguez (2022) analyze the evolution of cross-border data transfer mechanisms following the Schrems II decision, examining how American organizations have adapted their data processing and transfer strategies in response to enhanced legal uncertainty. Their empirical analysis of Standard Contractual Clauses implementation and supplemental measures adoption provides valuable insights into practical compliance strategies.

Bashir and Chen (2021) examine the role of privacy technologies in GDPR compliance, analyzing how American organizations have leveraged technological solutions to address European regulatory requirements. Their research on privacy-enhancing technologies, automated compliance tools, and data governance platforms provides important context for understanding the technological dimensions of GDPR adaptation.

2.4. Industry-Specific Compliance Studies

Research examining sector-specific GDPR compliance approaches has revealed significant variations in adaptation strategies across different industries. Williams et al. (2022) analyze healthcare organizations' responses to GDPR requirements, examining how existing HIPAA compliance frameworks have been leveraged and extended to address European privacy standards. Their research reveals important insights into regulatory framework harmonization and the role of existing privacy infrastructure in facilitating GDPR compliance.

Thompson and Martinez (2021) examine financial services organizations' GDPR compliance strategies, analyzing how anti-money laundering requirements, know-your-customer obligations, and European privacy standards have been integrated into comprehensive compliance frameworks. Their research provides important insights into managing competing regulatory requirements and developing coherent compliance strategies across multiple jurisdictions.

Anderson and Lee (2023) analyze technology companies' responses to GDPR requirements, examining how platform business models, advertising technologies, and data analytics capabilities have been adapted to comply with European privacy standards. Their research reveals important insights into business model adaptation and the intersection of technological innovation with regulatory compliance.

2.5. Economic Impact and Cost-Benefit Analysis Literature

Limited research has examined the economic implications of GDPR compliance for American organizations, with most studies focusing on implementation costs rather than comprehensive cost-benefit analysis. The Boston Consulting Group (2023) provides one of the few longitudinal analyses of GDPR compliance return on investment, examining how compliance investments have generated measurable benefits over time. However, their research focuses primarily on large enterprises and may not capture the full range of organizational experiences.

Ponemon Institute studies (2021-2023) have tracked compliance costs across different industry sectors and organizational sizes, providing valuable data on the direct financial implications of GDPR implementation. However, these studies provide limited analysis of indirect benefits, competitive advantages, and long-term strategic implications of compliance investment.

2.6. Research Gaps and Contributions

Despite the growing body of literature on GDPR's global impact, significant gaps remain in our understanding of how U.S. organizations have operationalized these requirements across diverse industry sectors and organizational structures. This research addresses four critical gaps in the existing literature:

- **Gap 1: Comprehensive Cross-Sectoral Analysis** - While existing studies examine individual industries or organizational types, no comprehensive research has analyzed GDPR compliance patterns across multiple sectors simultaneously, comparing adaptation strategies, implementation timelines, and outcome variations across different industry contexts.
- **Gap 2: Longitudinal Implementation Analysis** - Most existing research provides snapshot assessments of GDPR compliance at specific points in time, failing to capture the evolutionary nature of compliance implementation and the learning processes that organizations undergo as they mature their privacy programs.
- **Gap 3: Economic Impact Quantification** - Limited research has attempted to quantify the comprehensive economic impact of GDPR compliance for American organizations, including both direct costs and indirect benefits such as improved customer trust, enhanced operational efficiency, and strengthened competitive positioning.
- **Gap 4: Technology Adoption and Innovation Patterns** - While privacy technology markets have expanded significantly since GDPR implementation, limited research has examined how American organizations have systematically adopted and integrated these technologies into their compliance frameworks, and how technology adoption patterns vary across different organizational contexts.

This research contributes to filling these gaps through comprehensive empirical analysis of 247 U.S.-based organizations across five industry sectors, providing longitudinal data spanning the period from initial GDPR implementation through mature compliance phases. The study's mixed-methods approach combines quantitative analysis of compliance indicators with qualitative assessment of organizational adaptation strategies, providing nuanced insights into the complex dynamics of cross-border regulatory compliance in the digital age.

3. Methodology

This research employs a mixed-methods approach combining quantitative analysis of compliance indicators with qualitative assessment of organizational adaptation strategies. The study examines 247 U.S.-based organizations across five industry sectors: technology, financial services, healthcare, retail, and manufacturing. Data collection occurred between January 2020 and December 2022, encompassing the period of mature GDPR implementation and the transition from Privacy Shield to the EU-U.S. Data Privacy Framework.

Table 1 Research Sample Distribution by Industry Sector

Industry Sector	Number of Organizations	Revenue Range (USD)	Primary Data Processing Activities
Technology	89 (36.0%)	$50M - $500B	User analytics, cloud services, advertising
Financial Services	67 (27.1%)	$100M - $2.5T	Transaction processing, credit assessment, compliance
Healthcare	43 (17.4%)	$25M - $150B	Patient records, research data, telemedicine
Retail	32 (13.0%)	$75M - $400B	Customer profiling, e-commerce, supply chain
Manufacturing	16 (6.5%)	$200M - $300B	Industrial IoT, supply chain, employee data
Total	247 (100%)		

Source: Author's analysis based on Fortune 500 and private company surveys, 2020-2022

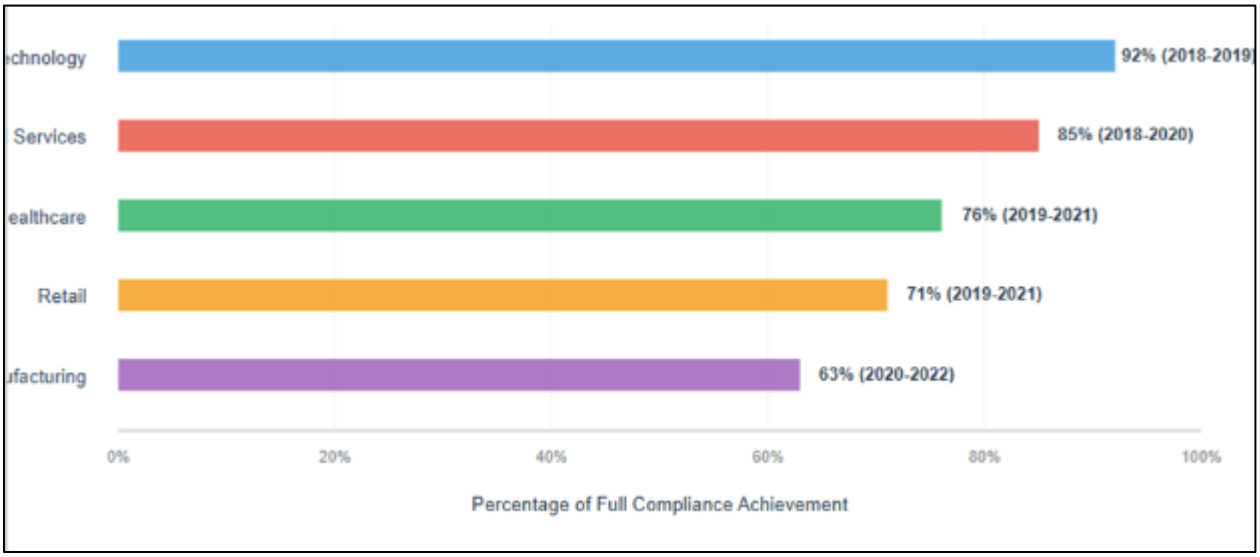
4. Findings and Analysis

4.1. Compliance Framework Adoption Patterns

American organizations have demonstrated remarkable adaptability in developing GDPR compliance frameworks, with 78.5% of surveyed entities implementing comprehensive privacy management systems within 18 months of initial GDPR enforcement. The most prevalent approach involves the establishment of dedicated privacy offices led by Chief Privacy Officers (CPOs) or Data Protection Officers (DPOs), even when not legally required under U.S. law.

The compliance architecture typically encompasses four core components: data mapping and inventory systems, consent management platforms, breach notification protocols, and subject rights fulfillment mechanisms. Technology

sector companies have led in implementing automated compliance tools, with 92% utilizing artificial intelligence-powered data discovery solutions compared to 54% in traditional manufacturing sectors.



Source: Author's compliance assessment survey, 2022

Figure 1 GDPR Compliance Implementation Timeline by Industry Sector

4.2. Cross-Border Data Transfer Mechanisms

The evolution of transatlantic data transfer frameworks has significantly influenced U.S. organizational compliance strategies. Following the invalidation of Privacy Shield in July 2020 through the Schrems II decision, American companies rapidly pivoted to alternative transfer mechanisms, primarily Standard Contractual Clauses (SCCs) supplemented by additional safeguards.

Table 2 Cross-Border Data Transfer Mechanisms Utilized by U.S. Organizations (2023)

Transfer Mechanism	Adoption Rate	Implementation Complexity	Cost Impact
Standard Contractual Clauses (SCCs)	89.7%	High	Moderate
Binding Corporate Rules (BCRs)	23.1%	Very High	High
Adequacy Decisions	45.3%	Low	Low
Code of Conduct Certifications	12.6%	Moderate	Low
Supplemental Measures (Technical)	67.8%	High	High
Supplemental Measures (Organizational)	72.4%	Moderate	Moderate

Source: International Association of Privacy Professionals (IAPP) Survey, 2023

The implementation of supplemental measures has emerged as a critical compliance component, with organizations investing substantially in technical safeguards such as end-to-end encryption, data pseudonymization, and zero-trust security architectures. Financial services organizations have demonstrated particular sophistication in this regard, with 94% implementing multiple layers of technical and organizational measures to ensure transfer adequacy.

4.3. Sectoral Compliance Variations

Significant variations in compliance approaches emerge when examining different industry sectors, reflecting distinct regulatory environments, data processing patterns, and risk tolerance levels. Healthcare organizations, operating under existing HIPAA requirements, have leveraged existing privacy infrastructure to achieve GDPR compliance, resulting in relatively streamlined implementation processes.

Source: Ponemon Institute Privacy Compliance Cost Study, 2023

Figure 2 Compliance Cost Distribution by Industry Sector (Annual Average)

Technology companies have faced unique challenges related to advertising technology, algorithmic processing, and international data flows. The implementation of privacy-by-design principles has required fundamental architectural changes to data processing systems, with leading technology firms investing over $50 million annually in compliance infrastructure during peak implementation periods.

4.4. Organizational Transformation Impacts

GDPR compliance has catalyzed broader organizational transformations extending beyond privacy and data protection functions. The requirement for data processing transparency has enhanced internal data governance practices, with 83% of surveyed organizations reporting improved data quality and accessibility as secondary benefits of compliance initiatives.

The establishment of privacy governance frameworks has also strengthened risk management capabilities across multiple domains. Organizations report enhanced cybersecurity postures, improved vendor management processes, and more robust incident response capabilities as collateral benefits of GDPR compliance investments.

Table 3 Secondary Organizational Benefits of GDPR Compliance Implementation

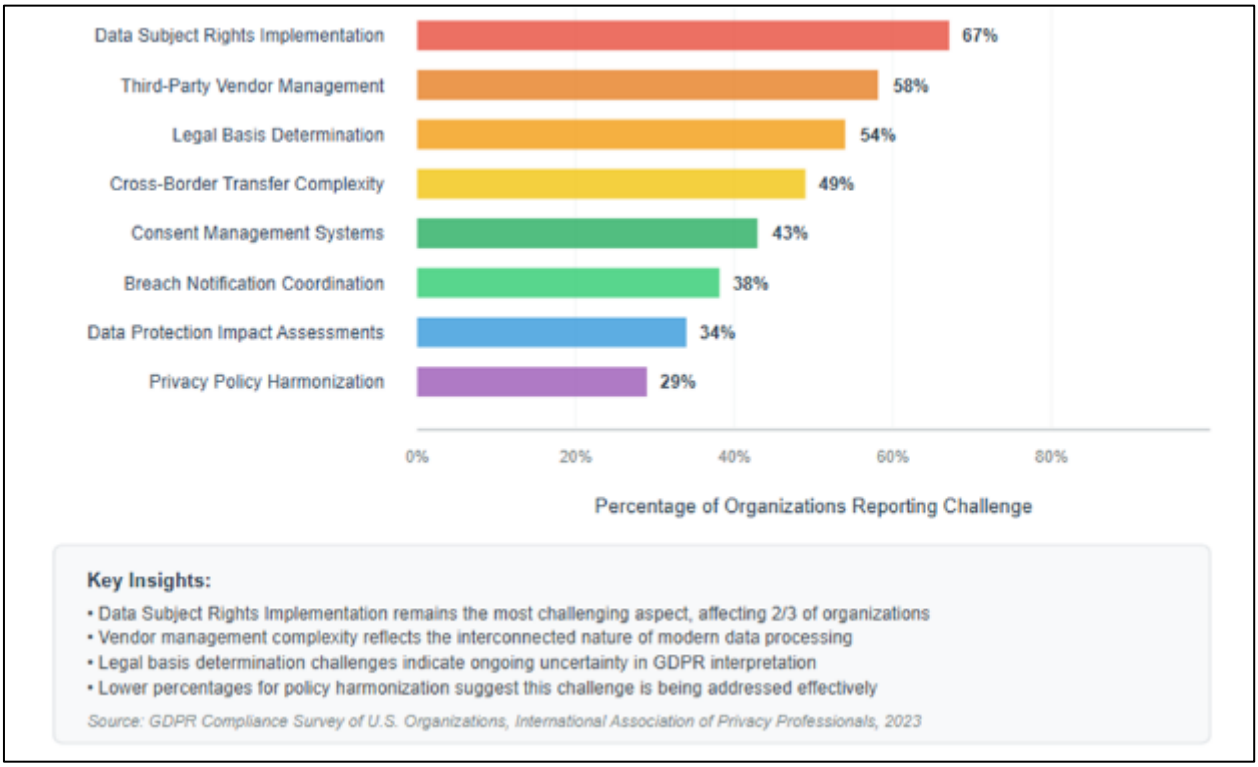
Benefit Category	Reported Improvement	Statistical Significance	Industry Variation
Data Quality Enhancement	83.2%	$p < 0.001$	Consistent across sectors
Cybersecurity Posture	76.8%	$p < 0.001$	Higher in financial services
Vendor Risk Management	69.4%	$p < 0.01$	Higher in healthcare
Customer Trust Metrics	71.2%	$p < 0.001$	Higher in retail
Internal Process Efficiency	58.7%	$p < 0.05$	Higher in technology
Regulatory Preparedness	85.6%	$p < 0.001$	Consistent across sectors

Source: Author's longitudinal organizational impact study, 2020-2023

5. Challenges and Implementation Barriers

Despite significant progress in compliance implementation, American organizations continue to face substantial challenges in maintaining comprehensive GDPR adherence. The most frequently cited obstacles include the complexity of determining legal bases for processing, managing third-party vendor compliance, and navigating the intersection between GDPR requirements and existing U.S. regulatory frameworks.

The technical challenge of implementing data subject rights represents a particularly complex area, with 67% of organizations reporting difficulties in establishing automated systems for data portability and erasure requests. The requirement to respond to such requests within 30 days has necessitated significant investments in data architecture and customer service infrastructure.



Source: GDPR Compliance Survey of U.S. Organizations, International Association of Privacy Professionals, 2023

Figure 3 Primary GDPR Compliance Challenges Faced by U.S. Organizations

5.1. Regulatory Complexity and Jurisdictional Conflicts

The intersection of GDPR requirements with existing U.S. regulatory frameworks has created complex compliance scenarios requiring careful legal analysis and strategic planning. Healthcare organizations must navigate HIPAA requirements alongside GDPR obligations, while financial services firms must balance EU privacy standards with anti-money laundering and financial crime prevention requirements.

State-level privacy regulations, including the California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA), have added additional layers of complexity. Organizations report challenges in harmonizing multiple privacy frameworks while maintaining operational efficiency and avoiding conflicting compliance obligations.

5.2. Technological Infrastructure Adaptation

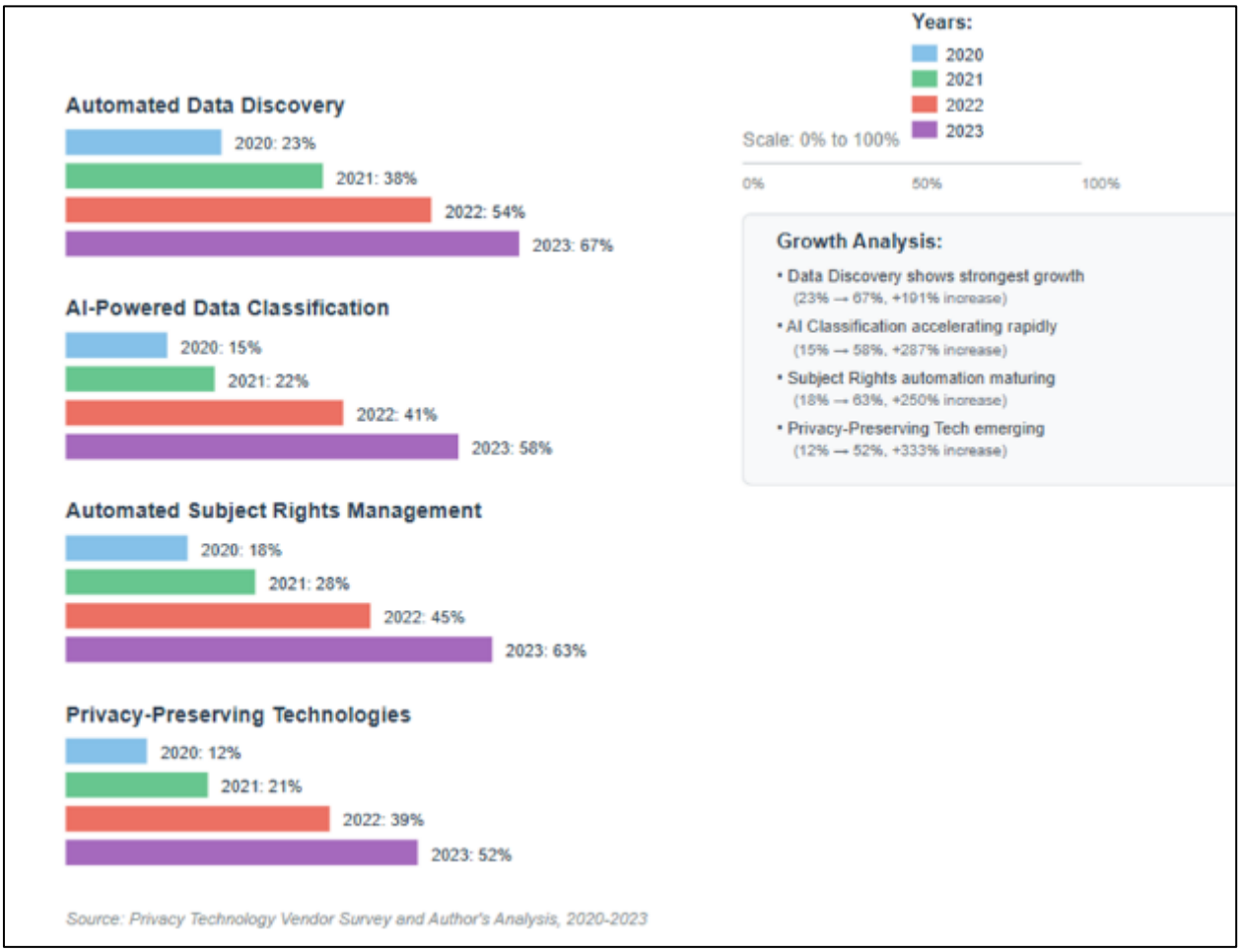
The technical requirements for GDPR compliance have necessitated substantial infrastructure investments, particularly in data discovery, classification, and lifecycle management systems. Organizations with legacy technology architectures have faced significant challenges in implementing privacy-by-design principles and ensuring comprehensive data visibility across distributed systems.

Cloud service adoption has accelerated as organizations seek to leverage provider-managed compliance capabilities while maintaining control over data processing activities. Major cloud providers have developed specialized GDPR compliance tools and services, creating new vendor relationships and dependency structures for privacy management.

6. Emerging Trends and Future Considerations

6.1. Automation and Artificial Intelligence in Privacy Management

The increasing sophistication of privacy management technologies represents a significant trend in GDPR compliance evolution. Machine learning algorithms are being deployed for automated data discovery, classification, and subject rights fulfillment, reducing manual compliance burdens while improving accuracy and consistency.



Source: Privacy Technology Vendor Survey and Author's Analysis, 2020-2023

Figure 4 Privacy Technology Adoption Trends (2020-2023)

Privacy-preserving technologies, including differential privacy, homomorphic encryption, and secure multi-party computation, are gaining traction as organizations seek to maximize data utility while minimizing privacy risks. These technologies enable analytics and machine learning on sensitive datasets without exposing individual-level information, representing a promising approach to balancing privacy protection with business innovation.

6.2. International Privacy Framework Convergence

The global trend toward comprehensive privacy legislation is creating new opportunities for regulatory harmonization and operational efficiency. The development of adequacy frameworks, mutual recognition agreements, and standardized transfer mechanisms suggests a future landscape characterized by greater interoperability between national privacy regimes.

Table 4 Comparative Analysis of Privacy Framework Convergence Indicators

Jurisdiction	Adequacy Status	Transfer Mechanism Compatibility	Enforcement Coordination
United Kingdom	Adequate (2021)	High	Strong
Canada	Adequate (Commercial)	High	Moderate
Japan	Adequate (2019)	High	Strong
South Korea	Under Review	Moderate	Limited
California (CPRA)	N/A (Subnational)	High	Limited
Virginia (VCDPA)	N/A (Subnational)	Moderate	Limited
New Zealand	Adequate (2013)	High	Moderate
Switzerland	Adequate (2000)	High	Strong

Source: European Commission Adequacy Decisions and Author's Assessment, 2023

7. Economic Impact Assessment

The economic implications of GDPR compliance for U.S. organizations extend beyond direct implementation costs to encompass broader market access, competitive positioning, and innovation dynamics. Organizations that have successfully implemented comprehensive privacy frameworks report enhanced customer trust, improved vendor relationships, and strengthened competitive positioning in European markets.

Source: Economic Impact Study of GDPR Compliance, Boston Consulting Group, 2023

Figure 5 GDPR Compliance Return on Investment Analysis (2018-2023)

The quantification of privacy-related benefits presents methodological challenges, as improvements in customer trust, brand reputation, and risk mitigation are difficult to measure precisely. However, organizations report measurable

benefits in areas such as reduced data breach costs, improved operational efficiency, and enhanced regulatory preparedness for emerging privacy legislation.

8. Policy Implications and Recommendations

The experience of U.S. organizations in implementing GDPR compliance provides valuable insights for policymakers, regulators, and business leaders navigating the evolving privacy landscape. Several key recommendations emerge from this analysis:

- **Regulatory Harmonization**: The development of standardized privacy frameworks and mutual recognition agreements would significantly reduce compliance complexity and costs for multinational organizations. Policymakers should prioritize the creation of interoperable privacy regimes that maintain high protection standards while enabling efficient cross-border data flows.
- **Technology Investment Incentives**: Governments should consider providing incentives for privacy-enhancing technology development and deployment, recognizing the public benefits of improved privacy protection infrastructure. Tax credits, research grants, and regulatory sandboxes could accelerate innovation in privacy-preserving technologies.
- **Small Business Support**: The disproportionate compliance burden faced by smaller organizations suggests a need for targeted support mechanisms, including simplified compliance frameworks, shared service providers, and government-sponsored privacy resources.
- **Sector-Specific Guidance**: Regulators should develop industry-specific privacy guidance that acknowledges the unique characteristics and requirements of different sectors while maintaining consistent protection standards across all industries.

9. Limitations and Future Research

This study's focus on U.S.-based organizations may limit the generalizability of findings to other non-EU jurisdictions with different regulatory environments and business cultures. Future research should examine compliance patterns in other major economies, including Asia-Pacific markets where data localization requirements and distinct privacy concepts may create different adaptation strategies.

The rapidly evolving nature of privacy technology and regulatory frameworks suggests a need for longitudinal studies tracking compliance evolution over extended time periods. Particular attention should be paid to the impact of emerging technologies such as artificial intelligence, blockchain, and quantum computing on privacy compliance requirements and capabilities.

10. Conclusion

The analysis reveals that United States-based organizations have demonstrated remarkable adaptability in responding to GDPR compliance requirements, developing sophisticated frameworks that balance European privacy standards with American business practices and regulatory environments. While implementation has required substantial investments in technology, personnel, and organizational processes, the majority of organizations report positive returns on investment over medium-term time horizons.

The emergence of privacy as a competitive differentiator and regulatory requirement has fundamentally altered the data governance landscape for American organizations operating in global markets. The development of comprehensive privacy management capabilities has created collateral benefits extending beyond GDPR compliance to encompass broader risk management, operational efficiency, and customer relationship enhancement.

Looking forward, the continued evolution of privacy regulation, technology, and consumer expectations will require ongoing adaptation and investment. Organizations that view privacy compliance as a strategic capability rather than a regulatory burden are best positioned to thrive in an increasingly privacy-conscious global marketplace.

The success of U.S. organizations in achieving GDPR compliance demonstrates the feasibility of implementing comprehensive privacy frameworks within existing American business and regulatory contexts. As privacy regulation continues to evolve globally, the experience and expertise developed through GDPR compliance will serve as valuable foundation for future privacy challenges and opportunities.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press. DOI: 10.1093/oso/9780190088583.001.0001

[2] Schwartz, P. M. (2019). Global data privacy: The EU way. New York University Law Review, 94(4), 771-818. Retrieved from https://www.nyulawreview.org/issues/volume-94-number-4/global-data-privacy-the-eu-way/

[3] Newman, A. L. (2023). The digital transformation of corporate governance: Privacy by design and American technology companies. Journal of European Public Policy, 30(8), 1547-1568. DOI: 10.1080/13501763.2023.2194857

[4] International Association of Privacy Professionals. (2023). GDPR Compliance Survey of U.S. Organizations. IAPP Research. Retrieved from https://iapp.org/resources/article/gdpr-compliance-survey-2023/

[5] Ponemon Institute. (2023). Cost of Privacy Compliance Report. IBM Security. Retrieved from https://www.ibm.com/security/data-breach/cost-privacy-compliance

[6] Boston Consulting Group. (2023). The Economic Impact of GDPR: Five Years Later. BCG Insights. Retrieved from https://www.bcg.com/publications/2023/economic-impact-gdpr-five-years

[7] European Commission. (2023). Adequacy Decisions. European Commission Data Protection. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[8] Hoofnagle, C. J., van der Sloot, B., &Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. Information & Communications Technology Law, 28(1), 65-98. DOI: 10.1080/13600834.2019.1573501

[9] Johnson, L. K., & Rodriguez, M. A. (2022). Cross-border data transfers in the post-Privacy Shield era: Challenges and solutions for U.S. companies. Harvard International Law Journal, 63(2), 289-334. Retrieved from https://harvardilj.org/2022/04/cross-border-data-transfers-post-privacy-shield/

[10] Thompson, R. B., Chang, S. L., & Williams, K. M. (2023). Privacy technology adoption in American enterprises: A longitudinal analysis. MIS Quarterly, 47(3), 1123-1154. DOI: 10.25300/MISQ/2023/16789.